DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO

(DPC)

TRUSTSIGN

1 AUTORIDADE CERTIFICADORA TRUSTSIGN

Declaração de Práticas de Certificação (DPC)
Última Revisão: 20 de outubro de 2010.
Versão 0.1
Publicado por: TrustSign

Histórico de Revisão
Versão: 1
Data: 20 de outubro de 2010
Autor inicial: Sthefane M Torres
Descrição das Mudanças: DPC Inicial

SUMÁRIO

1 INTRODUÇÃO 12
1.1 Visão Geral 12
1.2 Nome e Identificação de Documentos 13
1.3 Participantes de PKI 13
1.3.1 Autoridades Certificadoras (ACs) 14
1.3.2 Autoridades de Registro (ARs) 14
1.3.3 Assinantes 14
1.3.4 Terceiros de Confiança 14
1.3.5 Outros Participantes 15
1.4 Utilização do Certificado 15
1.4.1 Utilização Apropriada de Certificado 15
1.4.2 Utilizações Proibidas de Certificado 15
1.5 Administração da Política 15
1.5.1 Organização Administradora de Documento 16
1.5.2 Contato 16
1.5.3 Pessoa que Determina a Adequação Da DPC às Políticas 16
1.5.4 Procedimentos De Aprovação Da DPC 16
1.6 Definições e Siglas 17
2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO 17
2.1 Repositórios 17
2.2 Publicação das informações de certificados 17
2.3 Intervalo ou frequência da publicação 17
2.4 Controles de acesso nos repositórios 18
3 IDENTIFICAÇÃO E AUTENTICAÇÃO 18
3.1 Nomeação 19
3.1.1 Tipos de nomes 19
3.1.2 Necessidade de nomes significativos 19
3.1.3 Anonimato ou pseudonimato de assinantes 19
3.1.4 Regras para interpretação de vários tipos de nomes 20

3.1.5 Unicidade de nomes 20
3.1.6 Reconhecimento, autenticação e papel de marcas registradas 20
3.2 Validação inicial de identidade 20
3.2.1 Método para comprovar a posse de chave privada 20
3.2.2 Autenticação de identidade de uma organização 20
3.2.3 Autenticação de identidade de um indivíduo 21
3.2.4 Informação não-verificada de assinante 21
3.2.5 Validação da autoridade 21
3.2.6 Critérios para interoperação 22
3.3 Identificação e autenticação para solicitações de reemissão de chave 22
3.3.1 Identificação e autenticação para solicitações de reemissão de chave 22
3.3.2 Identificação e autenticação para solicitações de reemissão de chave após Revogação 22
3.4 Identificação e autenticação para solicitações de revogação 23
4 REQUISITOS OPERACIONAIS DE CICLO DE VIDA DO CERTIFICADO 23
4.1 Solicitação de Certificado 23
4.1.1 Quem pode submeter uma solicitação de certificado? 24
4.1.2 Processo de Inscrição e responsabilidades 24
4.2 Processamento de solicitação de certificado 25
4.2.1 Realização das funções de identificação e autenticação 25
4.2.2 Aprovação ou rejeição de solicitações de certificado 25
4.2.3 Tempo de processamento das solicitações de certificado 26
4.3 Emissão de Certificados 26
4.3.1 Ações da AC durante a emissão de certificados 26
4.4 Aceitação de certificados 26
4.4.1 Conduta de constituição de aceitação de certificado 26
4.4.2 Publicação do certificado pela AC 27
4.4.3 Notificação de emissão do certificado pela AC a outras entidades 27
4.5 Utilização de par de chaves e certificado 27
4.5.1 Utilização de chave privada e certificado pelo assinante 27
4.5.2 Utilização de chave pública e certificado por terceira parte 27
4.6 Renovação de Certificado 28

4.6.1 Circunstâncias para renovação de certificado 28
4.6.2 Quem poderá solicitar a renovação 28
4.6.3 Processamento de solicitações de renovação de certificado 28
4.6.4 Notificação da emissão de novo certificado ao assinante 29
4.6.5 Conduta de constituição da aceitação de certificado renovado 29
4.6.6 Publicação do certificado renovado pela AC 29
4.6.7 Notificação da emissão do certificado pela CA a outras entidades 29
4.7 Reemissão de chave de Certificado 29
4.7.1 Circunstâncias para reemissão de-certificado 29
4.7.2 Quem pode solicitar a certificação de uma nova chave pública 30
4.7.3 Processamento de solicitações de reemissão de certificado 30
4.7.4 Notificação da emissão de novo certificado ao assinante 30
4.7.5 Conduta de constituição da aceitação de certificado reemitido 30
4.7.6 Publicação de certificado reemitido pela AC 30
4.7.7 Notificação da emissão de certificado pela AC a outras entidades 30
4.8 Modificação do Certificado 31
4.8.1 Circunstâncias para a modificação de certificado 31
4.8.2 Quem poderá solicitar a modificação de certificado 31
4.8.3 Processamento de solicitações de modificação de certificado 31
4.8.4 Notificação de emissão de novo certificado ao assinante 31
4.8.5 Conduta de constituição de aceitação de certificado modificado 32
4.8.6 Publicação do certificado modificado pela AC 32
4.8.7 Notificação da emissão de certificado pela AC a outras entidades 32
4.9 Revogação e suspensão de certificados 32
4.9.1 Circunstâncias para revogação 32
4.9.2 Quem pode solicitar revogação 33
4.9.3 Procedimento para solicitação de revogação 33
4.9.4 Prazo para solicitação de revogação 33
4.9.5 Tempo de processamento da solicitação de revogação pela AC 34
4.9.6 Requisitos de verificação de revogação para Terceiros de Confiança 34
4.9.7 Freqüência de emissão de LCR 34
4.9.8 Latência máxima das LCRs 34

4.9.9 Disponibilidade para revogação ou verificação de status on-line 34
4.9.10 Requisitos para verificação de revogação on-line..... 35
4.9.11 Outras formas disponíveis para divulgação de revogação 35
4.9.12 Requisitos especiais para o caso de comprometimento de chave 35
4.9.13 Circunstâncias para suspensão 35
4.9.14 Quem pode solicitar suspensão 35
4.9.15 Procedimento para solicitação de suspensão..... 35
4.9.16 Limites no período de suspensão..... 35
4.10 Serviços de Status de certificados..... 36
4.10.1 Características operacionais..... 36
4.10.2 Disponibilidade do serviço 36
4.10.3 Recursos opcionais..... 36
4.11 Término da Assinatura 37
4.12 Recuperação e Guarda de chave..... 37
4.12.1 Políticas e Práticas de recuperação e guarda de chave 37
4.12.2 Políticas de práticas de Encapsulamento e recuperação de de Chave de Sessão 37
5 INSTALAÇÕES, GERENCIAMENTO E CONTROLES OPERACIONAIS..... 37
5.1 Controles Físicos..... 37
5.1.1 Construção e localização das instalações..... 38
5.1.2 Acesso Físico..... 39
5.1.3 Energia elétrica e ar condicionado..... 40
5.1.4 Exposição à água 40
5.1.5 Prevenção e proteção contra incêndio. 40
5.1.6 Armazenamento de mídia..... 40
5.1.7 Eliminação de resíduos..... 41
5.1.8 Backup em local externo 41
5.2 Controles de procedimento 41
5.2.1 Funções de Confiança da AC 41
5.2.2 Funções de Confiança da AR 42
5.2.3 Funções de Administrador de Sistema Operacional 42
5.2.4 Número de pessoas necessário por tarefa..... 42
5.2.5 Identificação e autenticação de cada função..... 43

5.2.6 Funções que exigem segregação de tarefas 43
5.3 Controles de Pessoal 43
5.3.1 Qualificação, Experiência e Requisitos de Idoneidade 44
5.3.2 Procedimentos de verificação de Antecedentes 44
5.3.3 Requisitos de treinamento 44
5.3.4 Freqüência e requisitos para reciclagem 44
5.3.5 Freqüência e seqüência de rodízio de trabalho 45
5.3.6 Sanções para ações não autorizadas 45
5.3.7 Requisitos para contratação de pessoal 45
5.3.8 Documentação fornecida ao pessoal 45
5.4 Procedimentos de registros de auditoria 46
5.4.1 Tipos de eventos registrados 46
5.4.2 Eventos Físicos 46
5.4.3 Eventos Lógicos 47
5.4.4 Requisitos de consolidação 48
5.4.5 Freqüência de auditoria de registros 49
5.4.6 Período de retenção para registros (log) de auditoria 49
5.4.7 Proteção de registro (log) de auditoria 49
5.4.8 Procedimentos para cópia de segurança (backup) de registro (log) de auditoria 50
5.4.9 Sistema de coleta de dados de auditoria (interno versus externo) 50
5.4.10 Notificação de agentes causadores de eventos 51
5.4.11 Avaliações de vulnerabilidade 51
5.5 Arquivamento de registros 51
5.5.1 Tipos de registros arquivados 51
5.5.2 Período de retenção para arquivos 52
5.5.3 Proteção de arquivo 52
5.5.4 Procedimentos de arquivamento de backups (cópias de segurança) 53
5.5.5 Requisitos para datação (time-stamping) de registros 53
5.5.6 Sistema de coleta de Arquivo (interno ou externo) 53
5.5.7 Procedimentos para obter e verificar informação de arquivo 53
5.6 Troca de-chave 53
5.7 Comprometimento e recuperação de desastres 54

5.7.1 Procedimentos a adotar em caso de incidentes e comprometimento 54
5.7.2 Recursos computacionais, software e dados corrompidos 54
5.7.3 Procedimentos de comprometimento de chave de entidade privada 55
5.7.4 Capacidades continuidade do negócio após um desastre 55
5.8 Extinção da AC ou da AR.....55
6 CONTROLES TÉCNICOS DE SEGURANÇA.....56
6.1 Geração e instalação do par de chaves 56
6.1.1 Geração de par de chaves 56
6.1.2 Entrega da chave privada ao assinantes 56
6.1.3 Entrega da chave pública para emissor de certificado 56
6.1.4 Entrega de chave pública da AC a Terceiros de Confiança 56
6.1.5 Tamanhos de chave.....57
6.1.6 Geração de parâmetros-de chave pública e verificação da qualidade 57
6.1.7 Geração de chaves da AC 57
6.1.8 Geração de chaves do Assinante.....57
6.1.9 Propósito de uso de chave (conforme o campo Key Usage X.509 v3).....57
6.2 Proteção de chave privada e Controles de Engenharia de Módulo Criptográfico.....58
6.2.1 Padrões de Controles de módulo criptográfico 58
6.2.2 Controle multi-pessoa (“n de m”) de chave privada.....58
6.2.3 Recuperação (scrow) de chave privada.....59
6.2.4 Cópia de segurança (back up) de chave privada 59
6.2.5 Arquivamento de chave privada 59
6.2.6 Transferência de chave privada de ou para um módulo criptográfico.....59
6.2.7 Armazenamento de chave privada em módulo criptográfico 59
6.2.8 Método de ativação de chave privada 60
6.2.9 Método de desativação de chave privada 60
6.2.10 Método de destruição de chave privada 60
6.2.11 Classificação de módulo criptográfico.....60
6.3 Outros aspectos do gerenciamento do par de chaves.....61
6.3.1 Arquivamento de chave pública.....61
6.3.2 Períodos operacionais do Certificado e períodos de utilização do par de chaves.....61
6.4 Dados de ativação 61

6.4.1 Geração e instalação dos dados de ativação 61
6.4.2 Proteção dos dados de ativação 61
6.4.3 Outros aspectos dos dados de ativação 62
6.5 Controles de segurança computacional 62
6.5.1 Requisitos técnicos específicos de segurança computacional 62
6.5.2 Classificação da segurança computacional 62
6.6 Controles técnicos do ciclo de vida 63
6.6.1 Controles de Desenvolvimento de Sistemas 63
6.6.2 Controles de gerenciamento de segurança 63
6.6.3 Controles de segurança do ciclo de vida 63
6.7 Controles de segurança de rede 64
6.8 Selo Cronológico 64
7 PERFIS DE CERTIFICADO, LCR E OCSP 64
7.1 Perfil do certificado 64
7.1.1 Número (s) de versão 64
7.1.2 Formato da base do certificado 64
7.1.3 Extensões de certificado 65
7.1.4 Certificados da AC 65
7.1.5 Identificadores de objeto de algoritmo 66
7.1.6 Formatos de Nome 66
7.1.7 Restrições de nome 66
7.1.8 OID (Object Identifier) de Políticas de Certificado 66
7.1.9 Uso da extensão "Policy Constraints 67
7.1.10 Sintaxe e semântica dos qualificadores de política 67
7.1.11 Semântica de processamento para a extensões críticas de políticas de certificado . 67
7.2 Perfil LCR 67
7.2.1 Número (s) de versão 67
7.2.2 LCR e extensões e entradas de LCR 68
7.3 Perfil OCSP 68
7.3.1 Número(s) de versão 68
7.3.2 Extensões de OCSP 68
8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES 68

8.1 Frequência e circunstâncias da avaliação 69
8.2 Identidade / qualificação do avaliador 69
8.3 Relação do Avaliador com a entidade avaliada 69
8.4 Tópicos cobertos pela auditoria 70
8.5 Medidas adotadas em caso de não-conformidade 70
8.6 Comunicação de resultados 70
9 OUTROS ASSUNTOS COMERCIAIS E JURÍDICOS 71
9.1 Tarifas 71
9.1.1 Tarifas de emissão e renovação de certificados 71
9.1.2 Tarifas de acesso ao certificado 71
9.1.3 Tarifas de revogação ou acesso à informação de status 71
9.1.4 Tarifas para outros serviços 71
9.1.5 Política de reembolso 72
9.2 Responsabilidade financeira 72
9.2.1 Cobertura de seguro 72
9.2.2 Outros ativos 72
9.2.3 Cobertura de seguro ou garantia para entidades 72
9.3 Confidencialidade de informações comerciais 73
9.3.1 Escopo de informações cofidenciais 73
9.3.2 Informação fora do escopo de informações confidenciais 74
9.3.3 Responsabilidade em proteger informações confidenciais 74
9.4 Privacidade da informação pessoal 74
9.4.1 Plano de Privacidade 75
9.4.2 Informações tratadas como privada 75
9.4.3 Informação não considerada privada 75
9.4.4 Responsabilidade em proteger informações privadas 75
9.4.5 Notificação e consentimento de uso de informações privadas 75
9.4.6 Divulgação por força de processo judicial ou administrativo 76
9.4.7 Outras circunstâncias de divulgação de informações 76
9.5 Direitos de propriedade intelectual 76
9.6 Representações e garantias 76
9.6.1 Representações e garantias da AC 77

9.6.2 Representações e garantias da AR 77
9.6.3 Representações e garantias do Assinante 78
9.6.4 Representações e garantias de Terceiros de Confiança 78
9.6.5 Representações e garantias de outros participantes 78
9.7 Isenção de responsabilidades 78
9.8 Limitações de responsabilidade 79
9.9 Indenizações 79
9.10 Prazo e terminação 80
9.10.1 Prazo 80
9.10.2 Terminação 80
9.10.3 Efeito de terminação e sobrevivência 80
9.11 Notificações individuais e comunicações aos participantes 81
9.12 Emendas 81
9.12.1 Procedimento para emendas 81
9.12.2 Mecanismo de notificação e período 81
9.12.3 As circunstâncias sob as quais o OID deve ser alterado 82
9.13 Procedimentos na Solução de Disputas 82
9.13.1 Negociação 82
9.13.2 Mediação 83
9.13.3 Arbitragem ou litígio 83
9.14 Leis Vigentes 83
9.15 Conformidade com a legislação aplicável 84
9.16 Disposições variadas 84
9.16.1 Contrato completo 84
9.16.2 Atribuição 84
9.16.3 Severidade 84
9.16.4 Aplicação (honorários advocatícios e renúncia de direitos) 85
9.16.5 Força maior 85
9.17 Outras disposições 85
10 GLOSSÁRIO 86

1INTRODUÇÃO

A TrustSign Comércio e Serviços em Tecnologia e Segurança da Informação (TrustSign) opera uma Autoridade Certificadora (AC). Este documento descreve o conjunto de normas e procedimentos estabelecidos pela Política da Autoridade Certificadora TrustSign para a operação da Autoridade Certificadora TrustSign .
Estruturado de acordo com a RFC 3647 [RFC3647], este documento descreve a política e as práticas dos serviços da PKI TrustSign. A Declaração de Práticas de Certificação (DPC) descreve as etapas que a TrustSign considera para implementar seus serviços de PKI em conformidade com as Políticas de Certificação da Raiz RSA. Estas duas declarações tomadas em conjunto são projetados para que uma Terceira Parte possa, ao observá-las, obter uma compreensão da fidedignidade das credenciais emitidas pela AC TrustSign.

1.1 Visão Geral

Esta Declaração de Práticas de Certificação (DPC) define as práticas e procedimentos para a criação de chaves para assinatura, assinatura e emissão de servidor web Secure Socket Layer (SSL) pela CA TrustSign. Esta DPC está em conformidade com a Política de Certificação da RSA Root Signing Service.
Esta DPC está em conformidade com a IETF PKIX Internet X.509 Public Key, com a PC e DPC da RSA (também conhecida como RFC 3647). Este documento está dividido em nove seções:
• Seção 1 - fornece uma visão geral da política e um conjunto de disposições, bem como os tipos de entidades e os aplicativos apropriados para os certificados.
• Seção 2 - contém quaisquer disposições aplicáveis em matéria de identificação da entidade ou entidades que operam repositórios, a responsabilidade de um participante PKI para publicar informações sobre as suas práticas, certificados, e a situação atual, a frequência de publicação e controle de acesso à informação publicada.
• Seção 3 - abrange os requisitos de identificação e autenticação de certificado para a atividade relacionada.
• Seção 4 - trata da gestão do ciclo de vida e os requisitos operacionais, incluindo requisição de certificado, revogação, suspensão, revisão de arquivamento, e do comprometimento de chaves.
• Seção 5 - abrange instalação, gestão e controles operacionais (requisitos de segurança física e processual).
• Seção 6 - fornece os controles técnicos em matéria de requisitos de criptografia de chave.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

• Seção 7 - define os requisitos para certificar os formatos da Lista de Certificados Revogados (LCR) e do Online Certificate Status Protocol (OCSP). Isso inclui informações sobre perfis, versões e extensões utilizadas.
• Seção 8 - aborda os temas tratados e a metodologia utilizados para as avaliações / auditorias; frequência de auditorias e avaliações; identidade e / ou qualificação do pessoal que executa a auditoria ou avaliação; ações tomadas como resultado de anomalias detectadas durante a avaliação, e que tem o direito de ver os resultados de uma avaliação.
• Seção 9 – coberturas gerais do negócio e questões jurídicas: honorários, responsabilidades, obrigações, requisitos legais, que regem as leis, processos, confidencialidade, etc.
A Política de Certificação (PC) do ROOT Signing Service da RSA descreve os requisitos legais, e técnicos do negócio para a AC TrustSign. A Declaração de Práticas de Certificação (DPC) descreve como estes requisitos são cumpridos na emissão de certificados SSL de servidor web. A AC TrustSign opera em São José dos Campos – São Paulo, Brasil.
Esta DPC não fornece detalhes sobre as operações da AC TrustSign, mas sim, fornece a visão geral das práticas. Detalhes das operações são encontrados em documentos adicionais.

1.2 Nome e Identificação de Documentos

O Object Identifier (OID) PC do Root Signing Service da raiz RSA é: 1.2.840.113549.5.6.1
Esta DPC está em conformidade com a PC do Root Signing Service (RSS) da RSA. Esta DPC é intitulada “Declaração de Práticas de Certificação da Autoridade Certificadora TrustSign” ou "DPC da AC TrustSign.

1.3 Participantes de PKI

Esta DPC é aplicável à AC TrustSign. As comunidades regidas por esta DPC são todos os componentes que residem dentro do ambiente de AC da TrustSign (por exemplo, Autoridades de Registro, Hardware Security Modules).
A AC TrustSign vai assinar e emitir certificados SSL para servidores web ou servidores de aplicação dentro da organização ou para organizações afiliadas que são de propriedade exclusiva da organização.
Esta DPC é aplicável a todos os certificados emitidos pela AC TrustSign. As práticas descritas nesta DPC são aplicadas à emissão, utilização e revogação dos certificados de Assinantes e Terceiros de Confiança da AC TrustSign.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

1.3.1 Autoridades Certificadoras (ACs)

A AC TrustSign opera sob a raiz das PC da RSA Root Signing Service que irá assinar os certificados SSL que ligam os assinantes (por exemplo, servidores web, servidores de aplicação) às suas chaves privadas. A AC é responsável por:

• Criar e assinar os certificados de ligação de assinantes com as suas chaves de verificação de assinaturas;
• Promulgar status do certificado através de publicação de certificados e LCR status aos repositórios acessíveis ao público; e
• A aderir a esta DPC e à raiz RSA, também se obriga a cumprir a PC (RSS).

1.3.2 Autoridades de Registro (ARs)

Não há ARs externas à entidade emissora. Somente a TrustSign (a autoridade de emissão) é responsável por todas as autorizações e as revogações de certificados.

1.3.3 Assinantes

Para efeitos da presente DPC, Assinante é uma entidade para a qual foi emitido um certificado SSL de servidor, um usuário/entidade final de Certificados emitidos pela AC TrustSign. .

A elegibilidade para um certificado é o critério utilizado pela AC TrustSign.

1.3.4 Terceiros de Confiança

Uma Terceira Parte é uma entidade que depende de um certificado ou de informações sobre o certificado emitido pela AC TrustSign.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

1.3.5 Outros Participantes

Não se aplica

1.4 Utilização do Certificado

Esta DPC é aplicável a todos os certificados emitidos e distribuídos pela AC TrustSign. As práticas descritas nesta DPC se aplicam à emissão, utilização e revogação dos certificados da AC TrustSign.

1.4.1 Utilização Apropriada de Certificado

Os certificados emitidos sob esta DPC pela AC TrustSign são adequados para:

• Proteger a integridade e autenticidade das transações comerciais através da implementação de SSL.

• Proteger a confidencialidade das informações para facilitar a transferência confidencial ou restringir o acesso a essas informações através da implementação de SSL.

O ponto 7.1.2 define ainda perfis de utilização do certificado.

1.4.2 Utilizações Proibidas de Certificado

Os certificados emitidos sob esta DPC pela AC TrustSign são proibidas em qualquer outro uso que o não especificado no item 1.4.1.

1.5 Administração da Política

A AC TrustSign é a autoridade administrativa global desta DPC.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

1.5.1 Organização Administradora de Documento

A AC TrustSign é a entidade responsável pela análise e aprovação de alterações a DPC. Comentários e propostas de alterações devem ser encaminhadas para o contato de Segurança da TrustSign conforme descrito na Seção 1.5.2. As decisões com relação às mudanças propostas estão a critério do Conselho de Segurança da TrustSign. A AC TrustSign é responsável pela elaboração, registro, manutenção e atualização desta DPC.

1.5.2 Contato

O contato à AC TrustSign deve ser direcionado a:

TrustSign Certificadora Digital e Representação Comercial Ltda.

Av. Alfredo Ignácio Nogueira Penido, n.300, cj 11, Jardim Aquárius – São José dos Campos, SP.

Telefone: (55) 12 3308 8420
(55) 11 3729 3945

Perguntas gerais podem ser enviadas para:

suporte@TrustSign.com.br

1.5.3 Pessoa que Determina a Adequação Da DPC às Políticas

O “RSA ROOT SIGNING SERVICE” (RSS) é a entidade administrativa que determina a adequação da DPC à “POLÍTICA DE CERTIFICAÇÃO” (PC) da RSA.

1.5.4 Procedimentos De Aprovação Da DPC

A autoridade que gerencia a Política de Segurança da TrustSign irá apresentar quaisquer alterações propostas para a DPC da AC TrustSign ao RSS da RSA. Revisões e determinação sobre estas alterações, acréscimos ou supressões são aceitáveis desde

que não prejudiquem as operações ou a segurança do RSS da RSA. Definições e Siglas podem ser consultadas no final deste documento uma lista de definições e acrônimos.

2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1 Repositórios

Os certificados TrustSign e sua LCR (Lista de Certificados Revogados) são publicados em um repositório remoto, como um diretório baseado em padrões LDAP. É responsabilidade da AC TrustSign publicar as seguintes informações em seu site (http://www.TrustSign.com.br):

- Sua DPC (disponível no site TrustSign e disponível quando necessário para fins de auditoria, acreditação ou certificação cruzada ou caso requisitado pela lei);
- Seus certificados;
- Todos os certificados emitidos pela AC TrustSign e seus respectivos status;
- A hierarquia da política de assinatura que constitui sua raiz;
- Sua lista de certificados revogados (LCR).

2.2 Publicação das informações de certificados

A AC TrustSign deve publicar informações sobre o status do certificado. A publicação dessas informações será dentro dos limites das seções 9.3 e 9.4. A publicação da LCR deve estar em conformidade com a seção 4. A AC irá publicar informações de status de certificados em intervalos frequentes, como indicado na DPC.

2.3 Intervalo ou frequência da publicação

As informações sobre os certificados serão distribuídas e / ou publicadas imediatamente após a emissão dos mesmos. Os prazos máximos e a frequência da publicações sobre o status dos certificados e a publicação da LCR estão descritos na seção 4 da presente DPC.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

2.4 Controles de acesso nos repositórios

As informações publicadas na Seção Repositório do Website da TrustSign são acessíveis ao publico geral com a finalidade de validar os certificados emitidos pela AC TrustSign pode limitar ou restringir o acesso aos seus serviços, como a publicação de informações de status de bancos de dados externos e pastas privadas.
Os controles de acesso podem ser instituídos para terceiros a critério da autoridade de certificação TrustSign respeitando o status do certificado. A AC TrustSign irá:

- Entregar os certificados imediatamente após a emissão dos mesmos;
- Fornecer diretamente ou de acordo com o repositório de acesso a LCR. A publicação da LCR ocorrerá de acordo com o ponto 4. Em alternativa ou adicionalmente, informações on-line do status do certificado será fornecido em conformidade com a seção 4;

- Incluir em qualquer certificado emitido, a URL do site mantido pela AC TrustSign ou emitido em seu nome;

- Providenciar a publicação desta DPC em um site mantido pela AC TrustSign, ou outra entidade em nome da AC TrustSign cuja localização será indicada de acordo com a seção 9.12;

- Fornecer uma única cópia de leitura desta DPC para publicação com medidas de segurança para assegurar que modificação não autorizada não ocorra;
- Fornecer texto integral da DPC, quando necessário, para efeitos de acreditação, auditoria ou conforme exigido por Lei.

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

Esta seção descreve os requisitos para a autenticação do solicitante do certificado. Nos casos em que o solicitante do certificado não for o proprietário do certificado, também descreve os requisitos para estabelecer quando o solicitante do certificado está autorizado a apresentar o pedido no nome do eventual proprietário do certificado.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

3.1 Nomeação

3.1.1 Tipos de nomes

Cada entidade terá um único e claramente distinguíveis nome distinto X.501 (DN) no campo assunto de acordo com o nome do certificado e em conformidade com PKIX Parte 1. Cada entidade só poderá usar um nome alternativo através do campo subjectalternatename, que também será de acordo com PKIX Parte 1. O DN estará na forma de um printablestring X.501, ia5string ou nome utf8 e não poderá constar em branco.

O subject name no certificado emitido pela AC TrustSign deve obedecer o nome distinto X.500 (DN) do formulário. A AC TrustSign deve usar uma convenção de nomenclatura única conforme descrito abaixo. Cada certificado SSL deve conter as seguintes informações:

• O "common name" (CN), que é o nome do host totalmente qualificado ou caminho usado no DNS do World Wide Web ou no servidor da TrustSign em que o certificado está instalado. A TrustSign deve ter direitos demonstráveis para o uso de qualquer nome de domínio que é um componente de um nome de domínio e/ou caminho totalmente qualificado.

3.1.2 Necessidade de nomes significativos

O conteúdo dos campos de nomes dos subject e issuer terão uma associação com o nome autenticado da entidade. O nome distinto relativo (NDR) deve refletir o nome legal autenticado da entidade ou nos casos em que a identidade do assinante é protegida, o nome poderá ser uma combinação de caracteres alfanuméricos.

3.1.3 Anonimato ou pseudoanonimato de assinantes

Em casos excepcionais, a identidade do assinante é protegida, o nome poderá ser uma combinação de caracteres alfanuméricos.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

3.1.4 Regras para interpretação de vários tipos de nomes

Não estipulado.

3.1.5 Unicidade de nomes

Nomes Distintos serão únicos para todos os assinantes. Quando os componentes de nomeação são semelhantes para os assinantes, números ou letras adicionais podem ser acrescentados para proporcionar unicidade (na maioria dos casos, o nome do assunto ou nome comum (CN)).

3.1.6 Reconhecimento, autenticação e papel de marcas registradas

O uso de marcas será reservado aos detentores da marca registada. O uso de um nome de domínio é restrito ao proprietário legal do Domain Name. A utilização de um endereço de e-mail deve ser restrita ao proprietário do endereço de e-mail.

3.2 Validação inicial de identidade

3.2.1 Método para comprovar a posse de chave privada

A AC TrustSign utiliza o método PKCS # 10 para comprovar a posse da chave privada.

3.2.2 Autenticação de identidade de uma organização

Para uma organização tornar-se Assinante, a AC TrustSign deve:

Verificar a cópia autenticada dos documentos da organização.
Verificar se o requerente é pessoa autorizada a agir em nome da organização (como descrito na seção 3.2.3).

Verificar o status de identidade e de trabalho da pessoa responsável pelo pedido e sua autoridade para receber as chaves para a organização.
Manter um registro dos detalhes da identificação utilizada e do tipo da identificação utilizada para a autenticação da organização, pelo menos durante a validade do certificado emitido.

3.2.3 Autenticação de identidade de um indivíduo

Um pedido de um indivíduo para ser um Assinante pode ser feito pelo próprio indivíduo, ou por outra pessoa ou organização legalmente autorizada a agir em nome do promitente Assinante.
A verificação da identidade e autenticação de um assinante pela AC TrustSign deverá ser feita através de pelo menos um dos meios abaixo:
Pessoalmente, em que a AC irá comparar a identidade do indivíduo com um documento de identidade com foto (cópias autenticadas ou originais), ou

On line, onde o Assinante concordará com os termos e condições de um Termo de Aceite. O Assinante preenche um formulário on-line e a AC realiza uma verificação de validação das informações apresentadas, ou

Se a AC TrustSign tiver um procedimento previamente estabelecido de verificação de identidade que satisfaça o RSS da RSA não houver nenhuma alteração nos dados apresentados, a TrustSign AC pode utilizar a informação privada partilhada (referido como um segredo compartilhado).

3.2.4 Informação não-verificada de assinante

Só as informações utilizadas para autenticar uma solicitação de certificado do Assinante serão verificadas; outras informações fornecidas pelo Assinante, como parte da inscrição não serão verificadas quanto à exatidão.

3.2.5 Validação da autoridade

A requisição de certificado deve ser feita por uma fonte individual ou independente que esteja vinculada e seja responsável pela entidade requisitante.

A AC TrustSign deve validar os seguintes itens de acordo com sua DPC:

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

A identidade do indivíduo que fez a requisição;

Verificar a existência da organização, de forma a validar a relação desta organização de negócios com a AC;

A autoridade do indivíduo para receber o certificado (s) em nome da organização.

Além disso, a AC TrustSign irá verificar se o nome de domínio no endereço de e-mail do requerente é o mesmo que o nome de domínio na solicitação de certificado.

3.2.6 Critérios para interoperação

Certificação cruzada entre ACs externas e a AC TrustSign não serão suportadas.

3.3 Identificação e autenticação para solicitações de reemissão de chave

3.3.1 Identificação e autenticação para solicitações de reemissão de chave

Antes da expiração de uma chave privada, um pedido de reemissão só pode ser realizado pela entidade em cujo nome as chaves tenham sido emitidas. A AC TrustSign deve autenticar todos os pedidos de reemissão e, a subsequente resposta será autenticada pela entidade a que foi emitido o certificado. Uma entidade que solicitou a reemissão pode autenticar o pedido usando uma assinatura digital gerada com a chave privada correspondente à chave pública certificada. Sempre que a chave privada de assinatura digital tiver expirado, o pedido de reemissão será autenticado da mesma forma como o registo inicial. Todos os casos de reemissão requerem a substituição da chave pública no certificado. Um novo par público/privado de chaves é gerado e um novo certificado é emitido.

3.3.2 Identificação e autenticação para solicitações de reemissão de chave após Revogação

Sempre que a informação contida em um certificado for alterada ou se houver comprometimento ou suspeita de comprometimento de chave privada, resultando em

uma revogação, a AC TrustSign deve autenticar uma reemissão do mesmo modo como ao registro inicial, nos termos do ponto 3.2. A AC TrustSign deverá verificar qualquer alteração das informações contidas em um certificado, antes que o certificado seja emitido.

3.4 Identificação e autenticação para solicitações de revogação

A AC TrustSign deve autenticar os pedidos de revogação de certificado. A AC TrustSign deve estabelecer o processo pelo qual abordará esses pedidos e os meios pelos quais irá estabelecer a validade do pedido. A AC TrustSign deve manter um registo do tipo e os detalhes do pedido de revogação incluindo a identificação e autenticação da pessoa solicitante.

O processo para o pedido de revogação segue abaixo:

1 - O cliente deve enviar e-mail solicitando e autorizando uma revogação do certificado.
2 - O pedido deve ser registrado como tarefa a ser realizada em qualquer sistema que possa ser auditado (Ex: CRM).
3 - Após a requisição ser registrada, ela deve ser encaminhada para a área responsável pelo processo de revogação.
4 - Após a revogação, o sistema deve ser atualizado e o cliente deve ser informado.
5 – O certificado de revogação pertencerá a uma Lista de Revogação de Certificados (LCR). Essa lista deverá ser publicada no site da TrustSign.

4 REQUISITOS OPERACIONAIS DE CICLO DE VIDA DO CERTIFICADO

4.1 Requisição de Certificado

Os procedimentos e exigências no que diz respeito à requisição de certificado são estabelecidos nesta DPC. Uma solicitação de certificado não obriga a AC TrustSign a emitir um certificado.
Existem três tipos principais de pedidos de certificados:

- Os Certificados da AC;
- Os Certificados de aplicação e de servidor web (SSL);
- Os Certificados de Administrador da AC, da AR e Vetor.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

O administrador do servidor web ou o operador irá apresentar uma solicitação de certificado PKCS # 10 através do processo de requisição de Certificado da AC TrustSign.

Solicitação de certificado web ou de servidor SSL

Uma entidade / pessoa autorizada a agir em nome de um departamento, organização ou grupo dentro da organização denominada “Assinante”, pode fazer uma solicitação para um certificado de servidor de aplicativos. As informações de contato administrativo serão identificadas, incluindo nome, cargo, endereço, telefone e e-mail. A solicitação de certificado seguirá os requisitos para as seções 3.2.2 a 3.2.3, bem como cumprirá os requisitos de qualquer acordo em vigor.

Solicitação de Certificado de administrador de AC, RA e Vetor

Solicitações de Certificado de administrador de AC, RA e Vetor serão apresentadas por uma entidade designada pelo AC TrustSign sendo necessário o cumprimento das exigências para o referido certificado. As informações de contato serão identificadas, incluindo nome, cargo, endereço, telefone e e-mail. O pedido seguirá os requisitos das seções 3.2.3.

4.1.1 Quem pode submeter uma solicitação de certificado?

Uma organização que tenha lido e aceito todas as exigências do DPC pode solicitar a emissão de um certificado. Os clientes da AC TrustSign devem ter um contrato assinado e válido entre eles e a AC, obrigando-os a cumprir todas as exigências descritas nesta DPC.
Qualquer informação do Assinante (ou seja, os dados necessários para a geração de um certificado ou de quaisquer dados para um repositório de dados fornecidos pelo assinante na página da inscrição) devem ser completos e validados com a divulgação integral de todas as informações exigidas no âmbito de uma requisição de certificado.

4.1.2 Processo de Inscrição e responsabilidades

Os Assinantes que registrarem e aceitarem o certificado da AC TrustSign serão obrigado a assinarem um Termo de Aceite ou acordo equivalente que consiste em:

• Constatação de que as informações de identificação fornecidas para a AC TrustSign durante o processo de inscrição prévio são verdadeiras e precisas

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

• Acordo para a proteção de chaves e senhas relacionadas ao certificado e, se aplicável, proteção dos tokens
• Acordo para o uso aceitável e confiável nos certificados conforme descrito na RSS da e CP da RSA e documentação de serviços relevantes da TrustSign;
• A obrigação de verificar a seleção de certificados corretos antes do uso;
• As obrigações e processos de revogação;
• Acordo sobre a validade dos certificados, e
• Outras renúncias previstas no acordo.

4.2 Processamento de solicitação de certificado

O Assinante deve estar vinculado às suas chaves públicas e informações apresentadas. A AC TrustSign devem exigir que cada pedido seja acompanhado de:

1. Prova de identidade e autorização para qualquer atividade relacionada ao certificado solicitado;
2. Acordo de assinante ou acordo de participação equivalente a termos e condições que regem as recorrentes utilizações do certificado, e
3. Uma requisição de certificado devidamente formatado em PKCS#10 ou equivalente, incluindo a chave pública.

4.2.1 Realização das funções de identificação e autenticação

A AC TrustSign ou RA associada em nome da CA, deve executar procedimentos de identificação e autenticação para validar um pedido de certificado.
Pedido de certificados de administrador de AC, administrador de AR, ou Vetor será apresentado por uma entidade designada pela AC TrustSign sendo necessário o cumprimento das exigências para o referido certificado. As informações de contato serão identificadas, incluindo nome, cargo, endereço, telefone e e-mail. O pedido seguirá os requisitos para a secção 3.2.3.

4.2.2 Aprovação ou rejeição de solicitações de certificado

Após a validação, a AC TrustSign notificará os Assinantes, diretamente ou através da RA associada, de que a AC criou o certificado, e disponibilizou ao assinante o acesso ao certificado. A AC pode emitir o certificado através de processos manuais ou automatizados.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

Um assinante será notificado por escrito ou por e-mail sobre um pedido de certificado rejeitado.

4.2.3 Tempo de processamento das solicitações de certificado

O período de tempo entre o recebimento de um pedido de certificado válido e a emissão e publicação deste certificado será no máximo de 24 horas.

4.3 Emissão de Certificados

4.3.1 Ações da AC durante a emissão de certificados

A AC TrustSign emite certificados com base nas solicitações que são correta e devidamente verificadas nos termos da Cláusula 3.1. A emissão de um certificado pela AC TrustSign indica a aprovação final e completa do pedido do certificado pela AC.

4.3.2 Notificações ao assinante pela AC emissora do certificado

Um assinante será notificado pela AC TrustSign da publicação do certificado do assinante em um repositório ou por confirmação de entrega do certificado do Assinante. A notificação de emissão será na forma de um e-mail ou uma mensagem (página web) para o assinante informando sobre a conclusão do processo de inscrição.

4.4 Aceitação de certificados

4.4.1 Conduta de constituição de aceitação de certificado

A AC TrustSign irá exigir que a entidade reconheça a aceitação do certificado SSL de servidor web. Haverá uma mensagem de aceitação "formal" da pessoa que está instalando os certificados SSL da Web no servidor Web como resposta à AC TrustSign.

4.4.2 Publicação do certificado pela AC

A AC TrustSign é responsável pelas funções de repositório e publicação. A AC TrustSign deve publicar certificados em um repositório baseado nas práticas de publicação de certificado da AC TrustSign, bem como informações sobre revogação de certificados, tal como definido no ponto 4.9 e 4.10.

4.4.3 Notificação de emissão do certificado pela AC a outras entidades

Nenhuma notificação de emissão ou de revogação será fornecido a qualquer outra parte, no caso de revogação, há a emissão de um LCR.

4.5 Utilização de par de chaves e certificado

4.5.1 Utilização de chave privada e certificado pelo assinante

O assinante só pode usar certificados emitidos pela AC TrustSign, e seus respectivos pares de chaves para os fins identificados no RSS, PC da RSA, e na DPC e em toda a documentação relevante da TrustSign. Os certificados e pares associados de chaves só podem ser utilizados para fins aprovados pela TrustSign.

4.5.2 Utilização de chave pública e certificado por terceira parte

Antes de usar um certificado de um assinante, a terceira parte deverá verificar se o certificado é apropriado para o uso pretendido.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

4.6 Renovação de Certificado

4.6.1 Circunstâncias para renovação de certificado

Renovação de certificado é a reemissão de um certificado com nova data de validade utilizando-se a mesma chave pública correspondente para a mesma chave privada. A renovação do certificado só será permitida em até 30 dias antes do vencimento do certificado. Em determinados casos, a renovação do certificado pode ser admitida quando as informações de um certificado foram alteradas.

4.6.2 Quem poderá solicitar a renovação

A AC TrustSign deve exigir que o assinante, entidade ou pessoa autorizada a agir em nome de um departamento, organização ou grupo, esteja em posse de um certificado válido e seja um funcionário ou agente com vínculo empregatício ou contrato com a empresa que cumpra com as disposições de emprego aplicáveis às políticas corporativas da TrustSign.
Qualquer informação adicional fornecida pelo Assinante deve ser completa e validada de forma integral como todas as informações requisitadas para a renovação de um certificado.

4.6.3 Processamento de solicitações de renovação de certificado

O Assinante deve ser estreitamente relacionado com suas chaves públicas e das informações apresentadas. A AC TrustSign deve exigir que cada renovação seja acompanhada por:
• Comprovante de identidade e autorização de todas as requisições de certificado, e
• Termo de Aceite ou um acordo equivalente a termos e condições de utilização do requerente do certificado.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

4.6.4 Notificação da emissão de novo certificado ao assinante

A notificação de emissão ocorrerá na forma de um e-mail ou uma mensagem (página web) para o assinante informando sobre a conclusão do processo de renovação.

4.6.5 Conduta de constituição da aceitação de certificado renovado

A AC TrustSign vai exigir que a entidade assine um Termo de Aceite de certificado de servidor SSL web. Haverá uma mensagem de aceitação "formal" da pessoa que está instalando os certificados SSL da Web no servidor Web como compromisso à AC TrustSign.

4.6.6 Publicação do certificado renovado pela AC

A AC TrustSign é responsável pelas funções de repositório e publicação. A AC TrustSign publica certificados, de acordo com o registro inicial, em um repositório baseado nas práticas de publicação de certificado da AC TrustSign, bem como informações sobre revogação de certificados, tal como definido no ponto 4.9 e 4.10.

4.6.7 Notificação da emissão do certificado pela CA a outras entidades

Nenhuma notificação de renovação será fornecida a qualquer outra parte, quando um certificado for renovado.

4.7 Reemissão de chave de Certificado

4.7.1 Circunstâncias para reemissão de-certificado

Rotina de reemissão de chave não é suportada. Antes que uma chave pública/privada expire, uma pessoa autorizada que represente o par de chaves pública/privada que está prestes a expirar será obrigada a fazer uma nova solicitação de certificado.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

4.7.2 Quem pode solicitar a certificação de uma nova chave pública

Não estipulado.

4.7.3 Processamento de solicitações de reemissão de certificado

Não estipulado.

4.7.4 Notificação da emissão de novo certificado ao assinante

Não estipulado.

4.7.5 Conduta de constituição da aceitação de certificado reemitido

Não estipulado.

4.7.6 Publicação de certificado reemitido pela AC

Não estipulado.

4.7.7 Notificação da emissão de certificado pela AC a outras entidades

Não estipulado.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

4.8 Modificação do Certificado

4.8.1 Circunstâncias para a modificação de certificado

Um certificado pode ser modificado:
1. Quando a base para qualquer informação no certificado for alterada.
2. Quando ocorrer uma mudança nas relações de negócio na qual o certificado foi emitido.

Quem poderá solicitar a modificação de certificado.

A modificação de um certificado somente poderá ser requerida por:
1. O indivíduo, departamento ou organização que fez o pedido de certificado em nome de uma organização ou um servidor de aplicação;
2. Um supervisor ou administrador autorizado (administrador delegado), em nome de um assinante; ou
3. Pessoal de emissão da AC TrustSign.

4.8.2 Processamento de solicitações de modificação de certificado

Todos os pedidos de alteração de certificado devem ser apresentados através de um processo on-line ou por escrito. O pedido de modificação autenticado e quaisquer ações resultantes tomadas pela AC TrustSign devem ser registradas e mantidas conforme necessário.

4.8.3 Notificação de emissão de novo certificado ao assinante

A notificação de emissão será na forma de um e-mail ou uma mensagem (página web) para o assinante, informando sobre a conclusão do processo de alteração/renovação.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

4.8.4 Conduta de constituição de aceitação de certificado modificado

A AC TrustSign vai exigir que uma entidade reconheça a aceitação do certificado de servidor web modificado. Haverá uma mensagem de aceitação "formal" da pessoa que está instalando os certificados SSL da Web no servidor Web como resposta à AC TrustSign.

4.8.5 Publicação do certificado modificado pela AC

A publicação de um certificado modificado ocorrerá conforme a publicação inicial do certificado.

4.8.6 Notificação da emissão de certificado pela AC a outras entidades

Nenhuma notificação de renovação será fornecida a qualquer outra parte, quando um certificado for modificado.

4.9 Revogação e suspensão de certificados

4.9.1 Circunstâncias para revogação

Um certificado será revogado:

1. Quando um Assinante não cumprir com as obrigações estabelecidas no RSS, na PC da RSA, nesta DPC, no Termo de Aceite ou na lei aplicável.
2. Quando a base para qualquer informação do certificado for alterada.
3. Quando ocorrer uma mudança nas relações de negócio sob a qual o certificado foi emitido.
4. Após suspeita ou comprometimento da chave privada, evidenciada por:

• Falta de dispositivos criptográficos.
• Evidente violação de selo ou envelope. Números ou datas e horários não concordarem com as entradas de log.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

• Selos de violação evidente ou envelopes abertos sem autorização ou que apresentem sinais de tentativas de abertura.
• Indicações de tentativas de acesso físico ou lógico no sistema de certificado por indivíduos ou entidades não autorizadas.
5. Quando um assinante não está mais participando da aplicação da AC TrustSign ou do serviço para o qual o certificado foi emitido, ou já não precisa de acesso a recursos organizacionais protegidos .
6. Quando a AC TrustSign suspeita que as condições podem levar a um comprometimento de chaves de um Assinante ou certificados, poderá, a seu critério, revogar o certificado de Assinantes.

4.9.2 Quem pode solicitar revogação

A revogação de um certificado só pode ser requerida:
1. Pelo indivíduo, departamento ou organização que fez o pedido de certificado em nome de uma organização ou um servidor de aplicação;
2. Um supervisor autorizado ou administrador (administrador delegado), em nome de um assinante ou
3. Pessoal da emissão da ACTrustSign

4.9.3 Procedimento para solicitação de revogação

Todos os pedidos de revogação devem ser apresentados através de um processo on-line ou por escrito. O pedido de revogação autenticado e quaisquer ações resultantes tomadas pelo AC devem ser registrados e mantidos conforme necessário. No caso de um certificado revogado, a justificativa para a revogação deve ser, também, documentada.
Sempre que um certificado de assinante for revogado, a revogação será publicada na LCR adequada da AC emissora TrustSign. A LCR será acessível de acordo com o ponto 4.9.

4.9.4 Prazo para solicitação de revogação

O período de carência de revogação ou prazo máximo disponível, no qual o assinante deve fazer um pedido de revogação em caso de suspeita de comprometimento é de 1 (um) dia útil. O período de carência não pode ultrapassar de um dia útil (ou seja, 8 horas de expediente).

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

4.9.5 Tempo de processamento da solicitação de revogação pela AC

O período de tempo entre o recebimento de um pedido de revogação do certificado e do processamento de um pedido de revogação de certificado será no máximo de um (1) dia útil (ou seja, 8 horas de expediente), porém uma ação imediata é o esperado.

4.9.6 Requisitos de verificação de revogação para Terceiros de Confiança

Antes de usar um certificado, uma terceira parte deverá verificar o status de todos os certificados da cadeia de validação de certificado contrapondo a LCR adequada e atual, em conformidade com os requisitos estabelecidos nos pontos 4.9 e 4.10. Como parte deste processo de verificação da assinatura digital, a LCR também será validada.
O acesso a LCR está na seguinte URL: www.TrustSign.com.br / LCR
Os pontos de distribuição da LCR serão identificados em cada certificado.

4.9.7 Frequência de emissão de LCR

A AC TrustSign emitirá uma LCR atualizada, pelo menos, a cada 30 dias. Nos casos em que um certificado SSL é revogado, a AC TrustSign emitirá uma nova LCR. A AC TrustSign irá sincronizar sua emissão e publicação de LCR para um diretório LDAP externo ou de publicação de servidor web para garantir que a LCR mais recente estará disponível para Partes de Confiança.

4.9.8 Latência máxima das LCRs

A AC TrustSign deve sincronizar automaticamente ou manualmente, a sua emissão de LCR com um diretório acessível ou site para proporcionar a acessibilidade da LCR mais recente para as Partes de Confiança. A latência para a publicação da LCR será imediata ou como a tecnologia de suporte puder gerenciar, geralmente em poucos minutos.

4.9.9 Disponibilidade para revogação ou verificação de status on-line

Não estipulado.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

4.9.10 Requisitos para verificação de revogação on-line

Não estipulado.

4.9.11 Outras formas disponíveis para divulgação de revogação

Não estipulado.

4.9.12 Requisitos especiais para o caso de comprometimento de chave

Não estipulado.

4.9.13 Circunstâncias para suspensão

A AC TrustSign não vai apoiar a suspensão de certificados SSL do servidor.

4.9.14 Quem pode solicitar suspensão

Não suportado pela AC TrustSign.

4.9.15 Procedimento para solicitação de suspensão

Não suportado pela AC TrustSign.

4.9.16 Limites no período de suspensão

Não suportado pela AC TrustSign.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

4.10 Serviços de Status de certificados

4.10.1 Características operacionais

A LCR terá como referência uma aplicação de PKI habilitado para verificar a validade de um certificado. Os certificados emitidos pela AC TrustSign incluem o nome e os pontos de distribuição da LCR como parte das informações de extensão do certificado. Quando um certificado é revogado ou expira, o número de série do certificado é adicionado à LCR.
A LCR Delta irá manter uma lista de certificados que foram revogados desde a última publicação da LCR Base. O cliente armazena em cache uma LCR base até o período de validade de a LCR expirar. Para garantir a validade de um certificado, o cliente deve receber a última lista de certificados revogados.
Quando um certificado é revogado, uma LCR será imediatamente publicada no diretório local do servidor ou web.
Imediatamente após a revogação, o banco de dados de repositório da AC é atualizado com as informações de revogação. Em uma base de exceção, as LCRs podem também ser emitidas entre estes intervalos (como a detecção de uma situação de grave comprometimento).

4.10.2 Disponibilidade do serviço

A AC TrustSign proporcionará uma LCR atual e acessível aos Terceiros de Confiança e aos assinantes para verificar o status de todos os certificados da cadeia de validação de certificado. A LCR será assinada para que a autenticidade e a integridade das LCRs possam ser verificadas.
O serviço estará disponível para consulta 24 horas por dia.

4.10.3 Recursos opcionais

Não estipulada.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

4.11 Término da Assinatura

O fim de uma assinatura (como resultante do término da necessidade do serviço ou de comprometimento) resultará na imediata revogação do certificado e da publicação de uma LCR ou de outro sistema de verificação de status de certificado.

4.12 Recuperação e Guarda de chave

4.12.1 Políticas e Práticas de recuperação e guarda de chave

A chave de assinatura privada da AC TrustSign não poderá ser recuperada. As chaves de assinatura privadas do Assinante não poderão ser recuperadas. As chaves privadas de criptografia de Assinantes poderão ser recuperadas. As chaves privadas serão recuperados através de exame e aprovação da AC TrustSign.

4.12.2 Políticas de práticas de Encapsulamento e recuperação de de Chave de Sessão

Não estipulado.

5 INSTALAÇÕES, GERENCIAMENTO E CONTROLES OPERACIONAIS

5.1 Controles Físicos

Os seguintes controles de segurança física devem estar em vigor antes da operação inicial do AC. Os assinantes devem satisfazer os requisitos de segurança, conforme documentado nesta DPC antes da emissão de certificado.
A AC TrustSign está alojada em um ambiente seguro, protegido por múltiplos níveis de segurança oferecendo suporte 7 dias por semana, 24 horas por dia. Aos profissionais são atribuídas responsabilidades de monitorar a segurança e a integridade das operações de serviços de PKI e de manter registos adequados, conforme necessário.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

5.1.1 Construção e localização das instalações

1. A AC TrustSign reside em um ambiente fisicamente seguro.
2. Com o objetivo de se proteger contra invasões, o ambiente fisicamente seguro é composto por:
• Gabinete de bloqueio para os sistemas de computação atuais, que exigem acesso de duas pessoas, que é usado exclusivamente para atividades relacionadas à emissão de certificados.
3. Uma ou mais câmeras de vigilância que fornecem um acompanhamento contínuo de entrada e saída para o ambiente fisicamente seguro. Câmeras de vigilância monitoraram as atividades dentro das instalações fisicamente seguras. Sob nenhuma circunstância as câmeras de vigilância serão configuradas para permitir o acompanhamento das telas de computador, teclados, PIN pads. Ativação da função de gravação ou será contínua ou será feita através de um detector de movimento, que é separado do sistema físico de detecção de intrusão. Iluminação contínua deve estar disponível para as câmeras.
4. O ambiente fisicamente seguro tem um sistema de detecção de intrusão:
• O sistema de detecção de intrusão tem vigilância 24 horas
• O sistema é capaz de gravar e arquivar a atividade de alarme.
• A Atividade de Alarme inclui tentativas de entrada não autorizada ou qualquer outra ação intencional ou acidental que desativa o sistema de detecção de intrusão.
• Todas as informações de atividade registrada de alarme serão analisadas e resolvidas.
5. A entrada ao “data center” requer pelo menos a utilização de cartões individuais de acesso de proximidade. As combinações necessárias para acesso físico do gabinete da AC física exigem pelo menos dois indivíduos autorizados.
6. Teclas físicas ou fechamentos de combinação são utilizados como mecanismo de controle de acesso:
• Teclas físicas para bloqueios devem ser marcados de forma que cada chave pode ser identificada, atribuída a um funcionário individual, controlados e auditados posteriormente, se necessário.
• A distribuição e recolhimento das chaves devem ser registadas. Um registro de acesso individual para cada chave será mantida em um banco de dados central ou repositório.
7. Quando um PIN ou uma senha é gravado, ela deve ser armazenada em um recipiente de segurança acessível apenas à pessoa autorizada.
8. Os sistemas de controle de acesso devem:
• Ser inspecionados, pelo menos trimestralmente por pessoal qualificado;
• A documentação de inspeção deve ser mantida por pelo menos um período de um ano para dar suporte aos requisitos de auditoria.
9. Todos os sistemas de controle de acesso e monitoramento devem ser ligados a uma UPS. O sistema UPS deve:
• Ser inspecionado, pelo menos anualmente;
• A documentação de controle deve ser conservada por um período mínimo de um ano.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

5.1.2 Acesso Físico

O acesso físico ao gabinete fisicamente seguro da AC relacionado ao sistema de dispositivos criptográficos deve ser limitado a pessoas autorizadas e um mínimo de controle para duas pessoas.
Pelo menos duas pessoas autorizadas devem estar presentes quando a AC for acessada.
Suportes de gravação ou imagens digitais devem ser solidamente mantidos por pelo menos 30 dias.
Procedimentos devem existir para a concessão e revogação de privilégios de acesso aos indivíduos.

Histórico de Segurança Física da AC

1. Logs de acesso devem ser revistos periodicamente e a revisão deve ser documentada.
2. Todos os acessos à emissão, revogação e procedimentos de revisão devem ser documentados.
3. O pessoal autorizado da AC (pessoas autorizadas com um papel formal PKI) deve assinar um diário de acesso (logbook). Este registro deve ser mantido no rack da AC. Este diário de acesso deve incluir:
• Data e hora de entrada e saída,
• Nome e assinatura do indivíduo,
• Organização participante,
• Motivo da visita.
4. Visitantes (empreiteiros, pessoal de manutenção, etc) para a instalação da AC devem ser acompanhados por pessoas autorizadas e assinar um diário de acesso. Este registro deve ser mantido dentro do rack da AC. Este diário de acesso deve incluir:

• Nome e assinatura do visitante,
• Organização participante,
• Nome e assinatura do indivíduo que acompanhou o visitante,
• Data e hora de entrada e saída,
• Motivo da visita.

5. Todos os eventos de emergência devem ser documentados. Sob nenhuma circunstância um indivíduo poderá omitir um evento de emergência em que foi envolvido.
6. O uso de qualquer entrada de emergência ou mecanismo de saída constitui evento de emergência.
7. Um processo deve existir para sincronizar a hora e data do acesso de detecção de intrusão e monitorização (câmara) de sistemas para assegurar a exatidão dos registros. Isso pode ser feito por qualquer mecanismo automático ou manual. Se um processo manual é utilizado, então o processo deve ocorrer pelo menos trimestralmente. A documentação da sincronização deve ser mantida por um período mínimo de um ano.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

Controles de Segurança Física do Assinante
Assinantes da TrustSign devem fornecer a proteção necessária para suas chaves privadas quando estas estiverem ou não em uso. As chaves privadas e secretas não devem estar em qualquer forma humana compreensível a qualquer pessoa em nenhum momento.
Assinantes, tais como servidor de aplicação, que contém as chaves privadas em um disco rígido (software gerado) devem ser fisicamente seguro ou protegidos com um nível de inicialização apropriado ou adequado de dois fatores de controle de acesso de autenticação.

5.1.3 Energia elétrica e ar condicionado

A AC TrustSign deve garantir que as instalações de condicionamento de energia e ar sejam suficientes para apoiar a operação do sistema de AC.

5.1.4 Exposição à água

A AC TrustSign deve assegurar que o sistema da AC seja protegido da exposição a água.

5.1.5 Prevenção e proteção contra incêndio.

A AC TrustSign deve assegurar que o sistema da AC seja protegido com um sistema de supressão de fogo.

5.1.6 Armazenamento de mídia

A AC TrustSign deve assegurar que os meios de armazenamento utilizados pelo sistema da AC sejam protegidos contra ameaças ambientais, como temperatura, umidade e magnetismo.

5.1.7 Eliminação de resíduos

A AC TrustSign deve assegurar que os meios de armazenamento utilizado pelo sistema da AC esteja protegido contra ameaças ambientais, como temperatura, umidade e magnetismo.

5.1.8 Backup em local externo

A AC TrustSign deve garantir que as instalações utilizadas para off-site back-up, se for o caso, tenham o mesmo nível de segurança como o site primário da AC.

5.2 Controles de procedimento

5.2.1 Funções de Confiança da AC

A AC TrustSign deve exigir uma separação das tarefas para funções críticas da AC para impedir a ação de uma pessoa de forma mal-intencionada através do sistema sem detecção da AC; prática referida como dividir conhecimento e duplo controle. O acesso de pessoal da AC aos sistemas da AC deve ser limitado a ações que sejam necessárias para executar o cumprimento das suas responsabilidades. Essas responsabilidades devem ser bem compreendidas pelo pessoal da AC.
Há uma separação de funções e controle de duas pessoas exigido para atividades específicas, tais como:
• Geração de novo par de chaves da CA;
• Substituição da chave de assinatura privada da CA e certificado de associado;
• Mudança no perfil da política de segurança de certificado (por exemplo, a renovação)
Todos os Administradores de AC e Vetores serão individualmente responsáveis por suas ações. Isto será realizado através de uma combinação de controles físicos, eletrônicos e de política:
• Acesso restrito às instalações – a entrada e saída serão monitoradas;
• Os logs de auditoria deverão gravar log-in e log-out de administrador do sistema operacional;
• Os logs de auditoria irão gravar log-in e log-out de administrador da AC;
• Os logs de auditoria registram emissão de certificados, revogação, etc (ver seção 5.4.1);
• Os controles técnicos que reforçam o acesso duplo;

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

• Política e controles processuais que exigem acesso duplo;

5.2.2 Funções de Confiança da AR

A AC TrustSign deve exigir que o pessoal da AR compreenda suas responsabilidades para a identificação e autenticação de assinantes potenciais e efetuar as seguintes funções:
1. A aceitação de pedidos de certificado, alterações de certificado e os pedidos de revogação de certificados;
2. A verificação da identidade e autorização de um assinante; e
3. Transmissão segura de informação do requerente para a AC TrustSign.

5.2.3 Funções de Administrador de Sistema Operacional

O sistema operacional que hospeda os sistemas da AC TrustSign deve exigir uma separação das tarefas por nível de sistema para impedir uma pessoa de ação maliciosa utilizando o sistema operacional de servidor da AC sem ser detectado. Os sistemas de acesso ao Administrador de Sistema Operacional devem ser limitados às ações necessárias para executar o cumprimento de suas responsabilidades. Essas responsabilidades devem ser bem compreendidas pelos Administradores de Sistema Operacional. O Administrador de Sistema Operacional não pode ser uma pessoa que também esteja preenchendo um papel de confiança na AC.

5.2.4 Número de pessoas necessário por tarefa

A AC TrustSign vai aplicar o princípio conhecido como "conhecimento dividido e controle duplo", de modo que nenhum indivíduo possa exercer individualmente atividades na AC. Em particular, a AC TrustSign deve implementar "n de m" de acesso. O "m" deve ser de pelo menos dois (2), e "n" não deve ser inferior a seis (6), no qual pelo menos duas pessoas são necessárias para iniciar uma ativação de assinatura de chave da AC.
Múltiplos controles de usuário são necessários para a geração de chaves da AC, conforme descrito na Seção 6.2.2.
A AC TrustSign deve ter um processo de verificação que fornece uma fiscalização de todas as atividades realizadas pelos titulares de função privilegiada na AC. Isso é, funções em que se possa emitir certificados, gerar chaves e administrar as configurações da AC.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

5.2.5 Identificação e autenticação de cada função

Todo o pessoal envolvido na operação da AC deve ter sua identidade e autorização verificada antes que eles sejam:
1. Incluído na lista de acesso para a instalação da AC;
2. Incluído na lista de acesso para o acesso físico ao sistema da AC;
3. Dado um certificado e conta para o desempenho de seu papel de funcionamento da AC; cada um desses certificados e as contas:
• São diretamente atribuíveis a um indivíduo;
• Não podem ser partilhados, e
• São restritos às ações autorizadas para o papel através do uso de uma combinação de software da AC, sistema operacional e controles processuais.
As operações da AC devem ser protegidas usando autenticação baseada em token e criptografia forte (isto é, smartcards).

5.2.6 Funções que exigem segregação de tarefas

A ACTrustSign deve exigir uma separação das tarefas para funções críticas para impedir uma pessoa de forma mal-intencionada através do sistema de AC sem detecção. Em particular, este é aplicável a todos os administradores da AC.

5.3 Controles de Pessoal

A AC TrustSign exige que todos os funcionários que exercem funções, no que diz respeito ao funcionamento de uma AC ou que estão interessados na gestão do AC, serão:
1. Nomeados por escrito;
2. Vinculados aos termos e condições do papel que estão a preencher;
3. Terão recebido formação adequada no que diz respeito aos deveres a serem desempenhados;
4. Obrigados a não revelar informações sensíveis e relevantes da AC para a segurança ou informações do Assinante; e
5. Não ter funções que possam causar conflitos com os seus deveres na AC.

5.3.1 Qualificação, Experiência e Requisitos de Idoneidade

A AC TrustSign exige que todos os funcionários que exerçam funções no que diz respeito ao funcionamento de uma AC tenham qualificação e experiência suficientes em PKI. Todo o pessoal deve cumprir os requisitos de organização pessoal e de segurança da AC. Os administradores devem ter o seguinte:

• Conhecimento e formação de PKI;
• Formação em Segurança;
• Formação específica nos produtos;
• Não constar antecedentes criminais na verificação de antecedentes.

5.3.2 Procedimentos de verificação de Antecedentes

Todas as verificações de fundo serão executadas em conformidade com o padrão de políticas e procedimentos organizacionais da TrustSign. Todo o pessoal contratado deve ser cuidadosamente selecionado por uma reputada agência de investigação:
• Verificação de antecedentes criminais;
• Históricos profissionais verificáveis;
Esse exame será repetido em uma base regular, não excedendo 10 anos.

5.3.3 Requisitos de treinamento

A AC TrustSign deve prever uma formação abrangente para todo o pessoal de PKI que exerçam funções no que diz respeito ao funcionamento da AC. Esse treinamento será composto de, no mínimo:

• Segurança de TI e conhecimentos gerais de PKI;
• Administração e funcionamento da AC; e
• Processos de recuperação de desastres da AC.

5.3.4 Frequência e requisitos para reciclagem

Os requisitos para a secção 5.3.3 devem ser mantidos atualizados para acomodar as mudanças em um sistema de AC (software e procedimentos). Treinamentos de

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

reciclagem devem ser realizados conforme o caso, e a gestão deve rever esses requisitos, uma vez por ano.

5.3.5 Frequência e sequência de rodízio de trabalho

No caso em que há rotatividade do emprego, todas as senhas poderão ser alteradas, ou os certificados necessários revogados e reemitidos, IDs de usu
ário que foram excluídas e recriadas. Não há compartilhamento de senhas ou contas.

5.3.6 Sanções para ações não autorizadas

Em caso de ação real ou suspeita de ação não autorizada por uma pessoa que exerça funções em relação ao funcionamento da AC TrustSign, a TrustSign suspenderá o acesso da pessoa à AC TrustSign imediatamente até que uma investigação seja conduzida. A critério da TrustSign e de seus executivos novas medidas podem ser recomendadas a respeito do status do emprego.
A AC TrustSign pode revogar todos os certificados aplicáveis quando um Assinante não cumprir com as obrigações previstas na RSS, CP e da RSA e desta DPC, qualquer acordo e/ou legislação aplicável. A AC TrustSign pode revogar um certificado, a qualquer momento se suspeitar que as condições podem levar a um comprometimento de chaves ou certificados.

5.3.7 Requisitos para contratação de pessoal

TrustSign limita o acesso do contratante ao site da AC TrustSign em conformidade com a Seção 5.3.

5.3.8 Documentação fornecida ao pessoal

A AC TrustSign colocará à disposição o seu pessoal o RSS, a PC da RSA e esta DPC e os procedimentos específicos, documentos e contratos relevantes para a sua posição. Isso inclui Procedimentos Operacionais Padrão, de Assinante, Planos de Recuperação de Desastres, e qualquer outro documento exigido pelo pessoal para desempenhar suas funções na AC.

5.4 Procedimentos de registros de auditoria

Arquivos de log de auditoria são gerados para todos os eventos relacionados à segurança da AC TrustSign. Sempre que possível, a auditoria de logs de segurança serão coletados automaticamente. Se isso não for possível, um diário de bordo, formulário de papel, ou outro mecanismo físico será utilizado. Todos os logs de auditoria de segurança, eletrônicos e não eletrônicos, serão mantidos e disponibilizados para as auditorias de conformidade e análise jurídica, se necessário por funcionários da lei.

5.4.1 Tipos de eventos registrados

Todos os eventos de segurança incluindo o tipo de acesso físico e lógico do processo, ou alterações de configuração, geração de chaves, criação de certificados, o uso da chave, e qualquer outro evento que possa ser necessário para fins de auditoria serão gravados. Os tipos de eventos são divididos em duas categorias:

• Eventos físicos, como sala de reforço, cofre e acesso;
• Eventos lógicos como as operações do sistema operacional e as operações do sistema da AC.

Eventos físicos podem usar gravação eletrônica e /ou diários de bordo. Monitoramentos de vídeo serão utilizados sempre que a presença física do pessoal de segurança não estiver disponível.
Eventos lógicos serão registrados automaticamente em logs de auditoria no nível operacional e nível de aplicação.

5.4.2 Eventos Físicos

Para os eventos de Física as seguintes informações serão registradas:

• Data e hora do evento;
• Identidade da entidade ou entidades;
• Finalidade de acesso (ou seja, manutenção, atualizações, melhorias, etc.);
• Todas as outras exigências que fornecem informações referentes ao evento (podem ser comentários sobre a substituição de uma unidade de disco, como resultado de uma falha).
Os seguintes eventos físicos serão registrados:
• Entrada da sala de acesso e saída;

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

• A ativação do alarme;
• Equipamento de sair e voltar; e
• Acesso ao sistema CA.

5.4.3 Eventos Lógicos

Eventos lógicos são divididos em sistema operacional e em eventos do sistema da AC. Todos os eventos lógicos deverão ser gravados na forma de um registro de auditoria conforme abaixo:
• Tipo de evento (aplicativo, sistema de segurança, etc)
• Data e hora de ocorrência do evento
• O sucesso ou fracasso do evento;
• Identidade da entidade e/ou do operador do CA que causou o evento; e
• Todos os detalhes sobre o evento (informações de erro ou informações de login) para eventual auditoria, e sempre que forem requisitadas. Os logs de auditoria deverão ser assinados digitalmente para manter a integridade das informações.

Sistema Operacional

Toda a atividade de login será registrada nos logs do sistema ou arquivo de log de acesso separado. Toda a atividade em nível de sistema (ao nível da raiz atividade ou equivalente) será registrada, conforme o caso, por uma instalação do sistema operacional ou o aplicativo de log de controle de acesso.
A seguinte lista representa os eventos de auditoria que serão monitorados no sistema operacional tanto para sucessos e fracassos:

• Eventos de logon, bem ou mal sucedidos;
• Uso de privilégios.
• Os eventos críticos do sistema.
• Eventos de emergência do sistema.
• Reinicialização do sistema.

Sistema da AC

Os seguintes eventos da AC serão monitorados e registrados nos casos de sucesso e falha:

• A geração de chaves
• Inscrição de um certificado de entidade final
• Inscrição de um certificado da AC
• Transferência de um certificado de entidade final a um cliente
• Transferência um certificado da AC para um cliente
• Download de um certificado para um cliente

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

- Geração de uma lista de revogação
- Importação de uma LCR
- Desistência de um certificado de entidade final
- Criação de uma AC
- Importação de um certificado da AC de PKCS12
- Criação um certificado administrativo
- Atualização de um certificado da AC
- Criação um certificado de assinatura
- Assinatura de um certificado de assinatura de código
- Reintegração de um Certificado da AC
- Suspensão de um Certificado da AC
- Revogação um Certificado da AC
- Suspenção de uma entidade final certificada
- Revogação de um certificado
- Revogação de um Certificado de assinatura de código
- Assinatura de um Certificado Cross Reverse
- Importação de um Certificado Avançado-Cross
- Revogação de um Certificado Cross Reverse
- Suspenção um Certificado Cross Reverse
- Reintegração de um Certificado Cross Reverse
- Eliminação de um Certificado Avançado-Cross
- Descarregamento de um Certificado Cross Reverse
- Eliminação de um registro de log de auditoria Secure Server
- Cópia de conteúdo de um log de auditoria Secure Login Server
- Mudança de papel de acesso de um certificado de entidade final
- Modificação de um ACL Web
- Modificação de uma ACL LDAP
- Aplicação de alterações na Jurisdição
- Aplicação de alteração de perfil em qualquer certificado
- Recebimento de uma solicitação de certificado
- Eliminação de um certificado de entidade final
- Backup completo do banco
- Backup de banco de dados elementares
- Backup do banco de arquivo de log transacional
- Emissão de um certificado de servidor CM
- Alteração do status de um pedido de certificado por um Vetor ou Administrador
- Inicialização de rastreamento
- Notificação de expiração de certificados

5.4.4 Requisitos de consolidação

As seguintes informação relativa à AC TrustSign serão coletadas, consolidadas e comunicadas eletronicamente ou manualmente:

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

• Sistema de mudanças de configuração e manutenção;
• Mudanças de pessoal;
• Divergências e relatórios de compromisso;
• Correspondência da AC com partes relacionadas externas, tais como software e hardware de fornecedores e prestadores de serviço no que se refere à manutenção do sistema;
• Destruição de meios contendo material de chaves, dados de ativação, ou informações pessoais do assinante.

5.4.5 Frequência de auditoria de registros

No mínimo, uma revisão dos registros de auditoria será realizada a cada 90 dias. Todos os eventos significativos deverão ser explicados em um resumo de log de auditoria. Tais revisões envolvem verificação de que o registro não foi adulterado e, em seguida brevemente inspecionar todas as entradas de log, com uma investigação mais aprofundada de quaisquer alertas ou irregularidades nos registros. Medidas tomadas na sequência dessas avaliações devem ser documentadas.
Estatisticamente, significativos conjuntos de dados de auditoria de segurança gerados pela AC TrustSign desde a última revisão serão examinados, bem como uma pesquisa razoável para qualquer evidência de atividade maliciosa.

5.4.6 Período de retenção para registros (log) de auditoria

A AC TrustSign deve manter a sua logs de auditoria por pelo menos 7 (sete) anos e irá reter logs de auditoria de forma descrita na Seção 5.5.2.

5.4.7 Proteção de registro (log) de auditoria

A configuração do sistema da AC TrustSign e os procedimentos serão implementados em conjunto para assegurar que:

• Somente pessoas autorizadas têm acesso de leitura aos registros;
• Somente pessoas autorizadas poderão arquivar ou apagar os logs de auditoria e,
• Os logs de auditoria não serão modificados.

O sistema de registro eletrônico de auditoria deve incluir mecanismos para proteger os arquivos de log quanto à visualização não autorizada, modificação ou eliminação. A

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

entidade de arquivo de log responsável pela realização de auditoria não deve ter direitos de modificação e serão implementados procedimentos para proteger os dados de auditoria arquivados no apagamento ou destruição antes do término do período de retenção do log de auditoria. Os logs de auditoria devem ser transferidos para um local de armazenamento seguro e separado do local da AC TrustSign primária.

As informações de auditoria manuais devem ser protegidas contra visualização não autorizada, modificação ou eliminação. Estes registos devem também ser colocados em uma área segura.

5.4.8 Procedimentos para cópia de segurança (backup) de registro (log) de auditoria

Devem ser feitos backup ou cópias dos logs de auditoria e os resumos de auditoria, conforme descrito no Plano de Recuperação e/ou Procedimentos Operacionais da AC, e colocados em uma área segura. Uma segunda cópia de todo o material retido ou backup serão armazenados em um local diferente do local primário da AC TrustSign e devem ser protegidos pela segurança física e/ou proteção criptográfica. Qualquer filial deve fornecer proteção adequada contra ameaças ambientais, como temperatura, umidade e magnetismo.

5.4.9 Sistema de coleta de dados de auditoria (interno versus externo)

A auditoria do sistema de coleta de logs será manual e automática. O sistema de coleta envolve a segurança física como parte da coleta de informações de auditoria. O acesso à sala, e ou recinto onde o sistema AC é armazenado e usado será monitorado. Parte do monitoramento pode ser gravado em vídeo.
Processos de auditoria do sistema operacional serão invocados na inicialização do sistema e permitirão apenas a operação de desligamento do sistema. Processos de auditoria da AC serão invocados na inicialização do aplicativo da AC e permitirão apenas o encerramento do aplicativo do sistema pela AC. Caso se torne evidente que um sistema de auditoria automatizada falhou, e que a integridade do sistema ou a confidencialidade das informações protegidas pelo sistema estão em risco, então a AC TrustSign deve determinar a suspenção das operações da AC até o problema ser sanado.

Sistema Operacional
- Log do Sistema
- Segurança registro do sistema operacional automática

AC Sistema
- Servidor Web logs

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

• Log Server: registro automático do software de Autoridade de Certificação

5.4.10 Notificação de agentes causadores de eventos

Quando um evento é registrado pelo sistema de coleta de auditoria, não é necessária nenhuma notificação à pessoa ou entidade que casou o evento.

Avaliações de vulnerabilidade

Eventos no processo de auditoria são registrados, em parte, para monitorar o comportamento inadequado, as vulnerabilidades do sistema e / ou compromissos. A AC TrustSign deve realizar uma avaliação de vulnerabilidade, fazer as recomendações apropriadas para resolver problemas e tomar as medidas adequadas, conforme necessário, na sequência de um exame desses eventos monitorados com base na frequência definida no ponto 5.4.2.

5.5 Arquivamento de registros

5.5.1 Tipos de registros arquivados

A AC TrustSign deve arquivar registros suficientemente detalhados para estabelecer o bom funcionamento da AC, ou a validade de qualquer certificado (incluindo os revogado ou expirado) emitido pela AC.
No mínimo, os seguintes dados devem ser gravados no arquivo:

• Geração de chave pública do AC TrustSign
• Declaração de Práticas de Certificação (cada versão)
• Obrigações Contratuais
• Sistema e configuração do equipamento
• Modificações e atualizações de sistema ou configuração
• As solicitações de certificado
• As solicitações de revogação
• Autenticação Assinante dados de identidade
• Documentação de recebimento e aceitação dos certificados
• Todos os certificados emitidos ou publicados
• Gravação de uma nova chave pública
• Todas as LCRs emitidas e / ou publicadas
• Todos os logs de auditoria

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

• Documentação exigida para cumprimento de auditoria

5.5.2 Período de retenção para arquivos

O período mínimo de conservação dos dados do arquivo é de um (1) ano a partir da data da sua criação. Informações específicas de cada cliente serão eliminadas de acordo com as normas de eliminação. Informações de auditoria e outras informações relativas às operações e continuidade do AC serão mantidas.

Se a mídia original não pode conservar os dados durante o período necessário, um mecanismo para transferir periodicamente os dados arquivados para a nova mídia a ser definida. Aplicações necessárias para processar os dados do arquivo também devem ser mantidas durante o tempo que for necessário, conforme determinado pela AC TrustSign.

5.5.3 Proteção de arquivo

Nenhum usuário não autorizado será permitido escrever, modificar ou excluir o arquivo. O conteúdo do arquivo não deve ser liberado, exceto como determinado pela AC TrustSign ou conforme exigido por lei. Registros de transações individuais podem ser liberados a pedido de quaisquer Assinantes envolvidos na operação ou seus representantes legalmente reconhecidos. Os arquivos de mídia devem ser armazenados em um cofre de armazenagem, seguro e separado do local da AC TrustSign.

O sistema de arquivamento automático deverá incluir mecanismos para proteger os ficheiros arquivados de visualização não autorizada, modificação ou eliminação.
Informações arquivadas de forma manual devem ser protegidas contra visualização de pessoas não autorizada, bem como sua modificação ou eliminação.

Os documentos que chegaram ao seu fim de vida serão destruídos conforme as regras adequadas com base na classificação do documento. Documentos em papel sensível ou confidencial serão triturados antes do descarte. Qualquer certificado, informações de auditoria ou de controle no papel serão considerados confidenciais e serão rasgado. Os documentos públicos podem ser colocados à disposição.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

5.5.4 Procedimentos de arquivamento de backups (cópias de segurança)

Dados de auditoria e cópias de segurança são enviados para serem protegidas em instalações de armazenamento off-site de acordo com os procedimentos de backup em um recipiente resistente ao fogo. Backup dos registros de arquivo são enviados para uma instalação de armazenamento seguro fora do local de longo prazo para o fim de armazenamento dos arquivos.

5.5.5 Requisitos para datação (time-stamping) de registros

Todos os documentos arquivados nos termos do presente ponto devem ser marcados com a data de sua criação ou execução.

5.5.6 Sistema de coleta de Arquivo (interno ou externo)

O sistema de recolha de arquivo será uma combinação de ambos os manuais e automáticas. O sistema de coleta envolve a segurança física como parte da coleta de informações de auditoria.

5.5.7 Procedimentos para obter e verificar informação de arquivo

A AC TrustSign deve verificar a integridade dos arquivos pelo menos uma vez a cada 12 meses.
O material armazenado fora do local também deve ser verificado pelo menos a cada 12 meses para a integridade dos dados.

5.6 Troca de-chave

A troca de chaves da AC TrustSign é baseada em obrigações contratuais. Se uma nova troca de chaves da AC TrustSign for necessária (por exemplo, devido ao vencimento), a AC deve gerar um novo par de chaves e apresentar o certificado para assinatura de ROOT Signing Service. O par de chaves antigo da AC deve ser removido e destruído. Haverá um período de transição para onde as chaves da AC TrustSign serão eliminadas

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

de forma progressiva. A chave privada da AC TrustSign não deve ser usada para assinar certificados emitidos com uma vida útil maior que a vida útil da chave privada da AC TrustSign.
Os subscritores só podem renovar o servidor web para criação de par de chaves SSL no prazo de um (1) mês antes da expiração da chave privada, que emite o certificado atual, não tendo sido revogada. Quando um certificado SSL para servidor web do assinante expira ou é infectado, um novo par de chaves será gerado e apresentado à AC TrustSign em relação ao aplicativo para substituir o certificado expirado. No caso de expiração do certificado ou comprometimento do servidor web o par de chaves deve ser removido do servidor web.

Pares de chaves sem validade devem ser re-autenticados pela TrustSign, em conformidade com os procedimentos na Seção 3.2. Quando um certificado de assinante foi revogado em virtude de não-conformidade com DPC da TrustSign, devem ser verificados os motivos da não-conformidade e se houve a readequação para as normas da DPC para nova remissão do certificado. Comprometimento e recuperação de desastres

Todas as informações específicas referentes à recuperação de desastres para a AC TrustSign serão fornecidas na PKI TrustSign Disaster Recovery Plan (DRP). O processo de recuperação será de acordo com o descrito na TrustSign DRP.

5.6.1 Procedimentos a adotar em caso de incidentes e comprometimento

Em caso de incidentes e comprometimento deverão ser seguidos os Procedimentos Internos de Operações da TrustSign.

5.6.2 Recursos computacionais, software e dados corrompidos

No caso da corrupção dos recursos computacionais, software e/ou dados, tal ocorrência é comunicada ao gestor responsável DRP TrustSign e procedimentos para lidar com incidentes devem ser promulgadas imediatamente. Esses processos requerem escalonamento adequado, a investigação de incidentes e resposta a incidentes. Se necessário, os processos de recuperação de desastres será promulgada.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

5.6.3 Procedimentos de comprometimento de chave de entidade privada

No caso improvável do comprometimento da chave privada associada com o certificado da AC TrustSign os seguintes passos devem ser seguidos:
• O ROOT Signing Service deve ser notificado assim que possível;
• Todos os inscritos serão notificados logo que possível, e
• Outras ações determinadas pelo ROOT Signing Service devem ser executadas.

O comprometimento da chave irá resultar no cancelamento imediato da assinatura.
A remissão será de acordo com o ponto 3.3.2.

5.6.4 Capacidades continuidade do negócio após um desastre

Uma autoridade de certificação deve fornecer procedimentos de continuidade de negócios em um Plano de Recuperação que delineiam os passos a serem tomados em caso de corrupção ou perda de recursos computacionais, software e / ou dados.

5.7 Extinção da AC ou da AR

No caso da CA TrustSign deixar de funcionar como uma autoridade de certificação:

• Todos os certificados emitidos pela CA serão revogados.
• Todas as entidades finais serão notificadas no prazo de 7 dias.
• Todas as chaves privadas de AC serão destruídas para impedir o comprometimento ou utilização fraudulenta.
• Um arquivo de banco de dados do CA será retido pelo serviço de PKI para um mínimo de sete (7) anos.
• A AC deve providenciar a retenção contínua de todas as chaves CA, LCR final e outras informações relevantes, tal como estipulado na secção 5.5.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

6 CONTROLES TÉCNICOS DE SEGURANÇA

6.1 Geração e instalação do par de chaves

6.1.1 Geração de par de chaves

A geração do par de chaves será a partir de uma criptografia Secure Hardware Security Module (HSM) nominal, pelo menos, FIPS PUB 140-2, nível 3. A geração de par de chaves será suportada em hardware ou software, conforme estipulado no ponto 6.1.6.

6.1.2 Entrega da chave privada ao assinantes

Não estipulado.

6.1.3 Entrega da chave pública para emissor de certificado

Todas as chaves públicas e certificados do Assinante serão armazenados no repositório da AC e/ou diretório LDAP. A entrega de chaves públicas deve estar de acordo com a PKCS # 10 Certificate Signing Request (CSR).

6.1.4 Entrega de chave pública da AC a Terceiros de Confiança

Todas as chaves públicas e certificados serão armazenados no repositório da AC e/ou diretório LDAP. As chaves públicas da CA TrustSign (como parte do seu certificado), e da cadeia de certificados de raiz associada à Raiz RSA Assinatura CA, devem ser entregues ao Assinante como parte do processo de emissão. O formato será de cadeia PKCS # 7 (binário ou base64), com. A assinatura de certificado da CA ROOT é pré-instalado no navegador web comum e o software de servidor web pelo fabricante do software.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

6.1.5 Tamanhos de chave

A AC TrustSign usará o algoritmo de criptografia RSA com um comprimento mínimo da chave de 2048 bits.
Os servidores web utilizarão algoritmo de criptografia RSA com uma duração mínima de chave de 1024 bits.

6.1.6 Geração de parâmetros-de chave pública e verificação da qualidade

6.1.7 Geração de chaves da AC

A assinatura de chaves da TrustSign AC deve ser gerada utilizando um processo aleatório ou pseudo-aleatórios, conforme descrito na norma ISO 9564-1 e ISO 11568-5 que são capazes de satisfazer os testes estatísticos de FIPS PUB 140-2, nível 3. As chaves da AC têm de ser protegidos por um módulo de hardware criptográfico classificado, no mínimo, o FIPS 140-2 Nível 3.

6.1.8 Geração de chaves do Assinante

Os assinantes irão gerar seu par de chaves de assinatura usando o software ou hardware de geração de chaves. No software, a geração do par de chaves usará o servidor web como ferramenta de geração de chave/aplicação (por exemplo, o Microsoft Certificate Wizard, ferramentas Apache). Se for utilizado hardware para a geração de chave (por exemplo, o acelerador de criptografia), o acelerador será avaliado em FIPS 140-2 Nível 2 ou maior. Sempre que possível, o par de chaves do SSL será gerado no servidor web que será instalado o certificado.

6.1.9 Propósito de uso de chave (conforme o campo Key Usage X.509 v3)

Consulte a seção 7 para o uso da chave como por Seção 7.1.1 e 7.1.2 certificados base e extensões de certificado.

A chave privada da AC TrustSign será utilizada apenas para assinar certificados de assinante e LCRs. O uso da chave será definido para a assinatura de certificado de chave e assinatura da LCR.

A chave privada do servidor web e e o certificado só serão utilizados para a autenticação do servidor web e criação de sessões SSL. O uso da chave será definido para assinatura digital e criptografia de chave. O uso prolongado de extensões de chave, se utilizado, será restrito a "Autenticação do Servidor".

6.2 Proteção de chave privada e Controles de Engenharia de Módulo Criptográfico

As chaves da AC devem ser protegidas por um módulo de hardware criptográfico seguro avaliado em FIPS 140-2, nível 3 ou superior.
O Assinante é responsável por sua chave privada e deve proteger sua chave privada de divulgação de acordo com os requisitos definidos por esta DPC. As chaves privadas só podem ser utilizadas para a finalidade prevista, tal como definido pelo perfil de certificados (seção 7) e do acordo de assinante.
A chave privada de um Assinante deve ser protegida contra o uso não autorizado por uma combinação de mecanismos de controle comercialmente razoáveis de criptografia e de acesso físico.

6.2.1 Padrões de Controles de módulo criptográfico

A AC TrustSign irá utilizar um HSM certificada FIPS 140-2 Nível 3 para proteger a chave de assinatura privada da AC. Assinantes (servidores Web) pode tanto guardar a chave de assinatura privada associada em software (por exemplo, registro da Microsoft) ou em um acelerador de criptografia de servidor SSL. O acelerador de criptografia SSL, se utilizado, será avaliado em FIPS 140-2 Nível 2 ou maior. Não há nenhuma exigência para qualquer HSMs para ser executada em "modo FIPS 'dentro dA AC TrustSign web ou aceleradores de servidor SSL de criptografia.

6.2.2 Controle multi-pessoa (“n de m”) de chave privada

Haverá controle de várias pessoas para as operações de geração de chaves da AC. No mínimo, deve haver várias pessoas o controle de procedimentos operacionais de tal forma que nenhuma pessoa pode ganhar o controle sobre a chave de assinatura da AC.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

O princípio do conhecimento dividido e controle duplo como definido no ponto 5.2.2, devem ser aplicadas.

6.2.3 Recuperação (scrow) de chave privada

Não haverá caução de chave privada em servidores de Web SSL.

6.2.4 Cópia de segurança (back up) de chave privada

O back-up de assinatura de chaves privadas da AC TrustSign será executado de forma segura para apoiar as operações de recuperação de desastre, conforme descrito no Disaster Recovery Plan (DRP) da AC TrustSign.
Os assinantes são responsáveis por fazer o backup da chave privada associada com a aplicação TrustSign e/ou certificados de serviço de forma segura (por exemplo, armários fechados, arquivo seguro, etc.).

6.2.5 Arquivamento de chave privada

As chaves privadas da AC TrustSign não serão arquivadas.

6.2.6 Transferência de chave privada de ou para um módulo criptográfico

Não estipulado.

6.2.7 Armazenamento de chave privada em módulo criptográfico

A chave de assinatura digital da AC deverá ser armazenada em um módulo de hardware criptográfico seguro pelo menos de FIPS 140-2 Nível 3.

6.2.8 Método de ativação de chave privada

Entidades devem ser autenticadas no módulo criptográfico antes da ativação da chave privada. Esta autenticação, no mínimo, será sob a forma de uma senha. Quando desativada, as chaves privadas devem ser mantidas de forma criptografada.

6.2.9 Método de desativação de chave privada

Quando as teclas são desativadas a aplicação deve limpar as chaves de memória antes de a memória ser deslocada. Qualquer espaço em disco, onde foram armazenadas as chaves deve ser sobrescrito antes que o espaço seja liberado para o sistema operacional. O módulo criptográfico deve desativar automaticamente a chave privada, após um período pré-definido de inatividade.

6.2.10 Método de destruição de chave privada

Após o término do uso de uma chave privada, sobrescrito com segurança deve destruir todas as cópias da chave privada na memória do computador e espaço em disco partilhado.

6.2.11 Classificação de módulo criptográfico

A geração de chaves da AC de assinatura digital, o armazenamento de assinatura digital e as operações de assinatura do certificado serão realizadas em um módulo de hardware criptográfico seguro pelo menos de FIPS 140-2 Nível 3.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

6.3 Outros aspectos do gerenciamento do par de chaves

6.3.1 Arquivamento de chave pública

A AC TrustSign mantém uma cópia de todos os certificados de servidor web SSL emitido dentro do banco de dados da AC. No banco de dados da AC é feito o backup e arquivado como parte das operações da AC. A AC TrustSign conservará por 7 anos todas as chaves públicas para verificação.

6.3.2 Períodos operacionais do Certificado e períodos de utilização do par de chaves

O período de uso da chave é de 2 (dois) anos, conforme estipulado no ROOT RSA assinatura do contrato com a RSA Security.

Os certificados SSL TrustSign serão emitidos com prazo de validade de um ano (1), dois anos (02) ou três anos (03). Períodos de utilização de chaves de Assinante será menor ou igual ao período remanescente de validade do certificado da AC TrustSign restante período de validade.

6.4 Dados de ativação

6.4.1 Geração e instalação dos dados de ativação

Não estipulado.

6.4.2 Proteção dos dados de ativação

Não estipulado.

6.4.3 Outros aspectos dos dados de ativação

Não estipulado.

6.5 Controles de segurança computacional

6.5.1 Requisitos técnicos específicos de segurança computacional

As seguintes funcionalidades, para a CA TrustSign, podem ser fornecidas pelo sistema operacional, ou através de uma combinação de sistema operacional, software da AC, e/ou física de salvaguardas (normas e procedimentos). O servidor da AC TrustSign deverá incluir as seguintes funcionalidades:

1. O controle de acesso aos serviços da AC e PKI papéis;
2. Forçados a separação de funções para funções de PKI;
3. Identificação e autenticação de papéis PKI e identidades associadas;
4. Uso de criptografia para comunicação sessão e segurança de banco de dados, autenticação mútua e sessões criptografadas são utilizados para todas as comunicações externas;
5. Arquivamento de AC e dados de histórico de entidade final e auditoria;
6. Auditoria de eventos de segurança;
7. Caminho confiável para a identificação das funções de PKI e identidades associadas, uso de certificados X.509 para todos os administradores e
8. Os mecanismos de recuperação de chaves e sistema da AC.

6.5.2 Classificação da segurança computacional

Não estipulado

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

6.6 Controles técnicos do ciclo de vida

6.6.1 Controles de Desenvolvimento de Sistemas

A AC TrustSign usa um software que foi concebido e desenvolvido sob uma metodologia de desenvolvimento formal. Um processo de verificação de integridade para assegurar a segurança do projeto e minimizar o risco residual deve apoiar o processo de concepção e desenvolvimento.
O Certificado de software de gestão utilizado usado por TrustSign segue a emissão do certificado e Gestão de Componentes (CIMC) Família de Proteção perfis que definem os requisitos para os componentes que emitir, revogar e gerenciar certificados de chave pública, tais como certificados de chave pública X.509. A CIMC é baseado no Common Criteria / IS15408 padrões ISO.

6.6.2 Controles de gerenciamento de segurança

Uma metodologia formal de gestão de configuração deve ser utilizada para instalação e manutenção permanente de um sistema AC. Software da AC, quando carregada pela primeira vez deve fornecer um método para uma AC para verificar se o software no sistema:
1. Foi originado a partir do desenvolvimento de software;
2. Não tenha sido alterado antes da instalação e
3. Seja a versão pretendida.
A AC TrustSign deve ter mecanismos comercialmente razoáveis e políticas para controlar e monitorar a configuração dos sistemas AC. Todas as mudanças ou modificações nos sistemas da AC necessitam de aprovação pelo Conselho de Segurança TrustSign Equipe de Gestão. O plano de gestão de configuração da AC TrustSign é detalhada nos Procedimentos Operacionais da AC TrustSign.

6.6.3 Controles de segurança do ciclo de vida

Não estipulado.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

6.7 Controles de segurança de rede

Os controles de segurança de rede permitirão apenas acesso autorizado ao servidor da AC TrustSign. Auditoria será ativada e marcada em uma base frequente. O acesso remoto ao ambiente da AC TrustSign será protegido por sessões autenticadas criptografadas. Nenhum outro acesso remoto é permitido para a plataforma de acolhimento para administração do sistema. Todos os serviços desnecessários serão desativados.

6.8 Selo Cronológico

O servidor da AC deverá sincronizar o seu relógio da máquina para o servidor NTP TrustSign. A exigência de datação de selos de dados é aplicável aos arquivos como descrito no capítulo 5.5.5.

7 PERFIS DE CERTIFICADO, LCR E OCSP

7.1 Perfil do certificado

7.1.1 Número (s) de versão

A AC TrustSign emite certificados X.509 Versão 3, em conformidade com o Certificado PKIX e perfil LCR.

7.1.2 Formato da base do certificado

A Base de certificado no formato estará de acordo com o padrão X.509. Os seguintes campos do certificado representam a base de suporte. Extensões adicionais são permitidas, se necessário.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

Certificado de Campo Descrição
Versão 3
Serial Number número de identificação único para este certificado atribuído pela CA TrustSign
Assinatura RSA com SHA-1
Emissora Domain Name (DN) (X.500) da emissão TrustSign CA
Validade de início e termo datas e horários do certificado
Assunto Domain Name (DN) (X.500) do sujeito, conforme ponto 3.1.1 desta DPC
Assunto informações de chave pública O valor da chave pública para o assunto, juntamente com um identificador do algoritmo com o qual esta chave pública é para ser usado

7.1.3 Extensões de certificado

7.1.4 Certificados da AC

A AC TrustSign apoiará a versão 3 extensões de acordo com RFC 3280 "Internet X.509 Public Key Infrastructure e Certificados perfil LCR.
O certificado da AC TrustSign é composto das seguintes extensões:

Field	Criticality	Description
Basic Constraint	Yes	Subject Type =CA; Path Length = 1
Authority Key Identifier	No	System Generated
Subject Key Identifier	No	System Generated
Certificate Policies	No	Identifies the Certificate Policy OID, URL and/or user notice; (PolicyIdentifier=1.2.840.113549.5.6.1)
LCR Distribution Point	No	Identifies how LCR information is published or obtained (URL and LDAP query).
Key Usage	Yes	Digital Signature (keyCertSign, LCRSign)

A CA TrustSign apoiará as seguintes extensões para certificados SSL: (The TrustSign CA will support the following extensions for web server SSL certificates:)

Field	Criticality	Description
Authority Key Identifier	No	System Generated
Subject Key Identifier	No	System Generated
Certificate Policies	No	Identifies the Certificate Policy OID, URL and/or user notice; (PolicyIdentifier=1.2.840.113549.5.6.1)

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

LCR Distribution Point	No	Identifies how LCR information is published or obtained (URL and LDAP query).
Key Usage	Yes	Digital Signature (digitalSignature); Key Encipherment (keyEncipherment)
Extended Key Usage	No	Server Authentication (serverAuth);
Subject Alternative Name	No	SubjectAltName: dNSname = (optional)

7.1.5 Identificadores de objeto de algoritmo

A AC TrustSign deve utilizar os seguintes algoritmos de apoio, para assinatura e verificação:

1. Algoritmo RSA de 1024 em conformidade com PKCS # 1 e / ou;
2. Algoritmo SHA-1, em conformidade com FIPS PUB 180-1 e ANSI X9.30 part2 e / ou;
3. Algoritmos adicionais apoiado pelo RSA Certificate Manager e SafeNet HSM.

7.1.6 Formatos de Nome

Cada DN deve ser na forma de um DirectoryString X.501. Os certificados emitidos por uma AC devem conter o nome distinto X.500 completo do emissor do certificado e sujeito do certificado no nome do emissor e campos de nome da entidade.

7.1.7 Restrições de nome

Sujeito e Emissora DNS devem respeitar as normas PKI e estar presente em todos os certificados.

7.1.8 OID (Object Identifier) de Políticas de Certificado

Política de Certificado de extensão será usado. O Object Identifier (OID) para a Política de Certificado correspondente ao certificado apropriado será conforme definido nesta DPC.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

7.1.9 Uso da extensão "Policy Constraints”

A AC TrustSign suporta o uso da extensão "Policy Constraints”.

7.1.10 Sintaxe e semântica dos qualificadores de política

A AC TrustSign preenche certificados X.509 Versão 3 com um qualificador de política dentro da extensão de Políticas de Certificação. Geralmente, esses certificados contêm um qualificador DPC que aponta para o aplicável TrustSign CA DPC.

7.1.11 Semântica de processamento para a extensões críticas de políticas de certificado

Extensões críticas, quando aplicável, devem ser interpretadas como definido no PKIX.

7.2 Perfil LCR

7.2.1 Número (s) de versão

A AC TrustSign emitirá LCRs X.509 versão 2, em conformidade com a RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.
A seguir representa os campos LCR base suporte.
Campo Descrição
Versão 2
Algoritmo de Assinatura O algoritmo identificador do algoritmo usado para assinar a LCR.
Nome da Emissora: identifica a entidade que assinou e emitiu a LCR.
Esta atualização: Este campo indica a data de emissão deste LCR.
Próxima Atualização: A data em que o LCR próxima será emitido.
Os certificados revogados: Certificados Revogados estão listados, a menos que não há certificados revogados, caso em que o campo está ausente

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

7.2.2 LCR e extensões e entradas de LCR

Todos entidade de software de PKI deverão processar corretamente todas as extensões de LCR necessária na parte PKIX um certificado e perfil LCR.
A AC TrustSign irá apoiar e utilizar a LCR, Versão 2 extensões:
Extensão LCR:
Descrição do campo Criticidade
Autoridade identificador de chave n º Fornece um meio de identificação de chave pública da CA que corresponde à chave privada usada para assinar a LCR.
LCR Number Nenhuma LCR extensão Número especifica um número seqüencial para cada LCR emitida pela AC.
LCR Extensão de entrada:
Descrição do campo Criticidade
Motivo Código n º Identifica a razão para a revogação do certificado; extensão omitido se o código de razão é desconhecida.
A prorrogação da data de invalidez entrada Date fornece a data em que se suspeita que a chave privada foi comprometida.

7.3 Perfil OCSP

7.3.1 Número(s) de versão

Não estipulado.

7.3.2 Extensões de OCSP

Não estipulado.

8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

Uma auditoria de conformidade constitui um atestado terceiro independente que a AC TrustSign está operando como indicado no RSS RSA PB e esta DPC. A AC TrustSign deve

ter uma auditoria de conformidade realizada às suas expensas para demonstrar a conformidade com o RSS RSA CP.

8.1 Frequência e circunstâncias da avaliação

Uma auditoria de conformidade será realizada seis meses após a emissão do Certificado PKCS # 7 da Raiz RSA de assinatura de serviços e cada 12 meses, conforme necessário, como parte do contrato para usar o RSA ROOT a assinatura de serviço.
A auditoria anual deverá determinar se o desempenho funcional (práticas de negócios e controles) da AC TrustSign atende aos requisitos do RSS RSA CP, e esta DPC. (A auditoria anual do cumprimento será determinar se a AC TrustSign desempenho funcional (práticas de negócios e controles) atende aos requisitos do RSS RSA CP, e esta DPC).

8.2 Identidade / qualificação do avaliador

O auditor tem de demonstrar competência no domínio das auditorias de conformidade, e deve estar totalmente familiarizado com os requisitos que o ROOT Signing impõe sobre a emissão e gestão de todos os certificados, e que TrustSign impõe sobre a emissão e gestão dos seus certificados. O Auditor de Conformidade deve realizar auditorias de conformidade com uma responsabilidade primordial.
O cumprimento da auditoria será independente da AC TrustSign e terá credenciais para identificar positivamente o Auditor Conformidade como pertencentes a uma empresa de auditoria reconhecida

8.3 Relação do Avaliador com a entidade avaliada

Para tanto o ROOT RSA assinatura de serviço e CA TrustSign, o auditor deve ser uma empresa privada, que é independente da entidade auditada, ou ele deve ser suficientemente organizacionalmente separada da entidade para fornecer uma avaliação imparcial, independente e de certificação. A RSA ROOT a assinatura de serviço deve determinar se um Compliance Auditor atende a esse requisito.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

8.4 Tópicos cobertos pela auditoria

A auditoria de conformidade cobrirá todos os requisitos que definem o funcionamento de um CA no âmbito do presente DPC, incluindo:

- TrustSign negócios CA divulgação práticas
- A RSA ROOT CONTRATAÇÃO DE SERVIÇOS integridade (chave e certificado de gestão do ciclo de vida)
- CA controles ambientais.

8.5 Medidas adotadas em caso de não-conformidade

Quando o Auditor encontra uma discrepância entre como TrustSign CA é projetado, sendo operado ou mantido, e os requisitos desta DPC eo RSA RSS CP, as seguintes ações podem ser tomadas dependendo da gravidade da discrepância / discrepâncias:

• Se a diferença for menor, o Auditor Conformidade deve observar a discrepância, como parte do relatório de auditoria de conformidade;

• Se a discrepância é de uma magnitude de negar uma auditoria de conformidade com sucesso, o Auditor Compliance reúne-se com A AC TrustSign Equipa de Gestão de imediato. A AC TrustSign vai determinar a forma de sanar a discrepância e discutir com o Compliance Auditor se o remédio é suficiente para obter ou manter a aprovação auditoria de conformidade. Conforme acordado TrustSign, RSA Security eo Auditor Compliance, um plano de ação com um cronograma distintos para a execução do remédio e um relatório final detalhando a discrepância remédio, eo resultado final será necessária. A decisão final pelo Auditor cumprimento será obrigatório e se, no julgamento do auditor Compliance, a discrepância é ainda grave, a auditoria de conformidade será considerado um fracasso.

• Se, na opinião do Auditor Conformidade dA AC TrustSign não está em conformidade com o RSS RSA CP, a RSA ROOT a assinatura de serviço pode, a seu critério, revogar o certificado da AC TrustSign, dependendo da gravidade do incumprimento .

8.6 Comunicação de resultados

O Compliance Auditor irá produzir um Relatório de Auditoria de Conformidade. O relatório de auditoria de conformidade será utilizada pelA AC TrustSign para demonstrar uma boa capacidade em suas práticas e procedimentos. O Relatório de Auditoria de Conformidade serão liberados para o ROOT RSA assinatura de serviço como uma comprovação da reunião anual da auditoria de conformidade. Todos os relatórios de auditoria incluem medidas correctivas continuará a ser propriedade exclusiva dA AC

TrustSign e serão tratados como confidenciais e protegidas em conformidade. Os resultados não serão tornados públicos a menos que exigido por lei ou por um acordo contratual entre a empresa e TrustSign ser dado acesso ao relatório.

9 OUTROS ASSUNTOS COMERCIAIS E JURÍDICOS

9.1 Tarifas

O TrustSign CA raiz não cobra taxas de seus serviços.

9.1.1 Tarifas de emissão e renovação de certificados

Não estipulado.

9.1.2 Tarifas de acesso ao certificado

Não estipulado.

9.1.3 Tarifas de revogação ou acesso à informação de status

Não estipulado.

9.1.4 Tarifas para outros serviços

Salvo disposição em contrário na outra relação contratual, TrustSign será responsável por todas as despesas administrativas relacionadas com o funcionamento dA AC TrustSign incluindo auditoria de conformidade nos termos do ponto 8 do presente documento.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

9.1.5 Política de reembolso

Não estipulado.

9.2 Responsabilidade financeira

TrustSign CA mantém níveis adequados de seguro necessárias para apoiar suas práticas comerciais.

9.2.1 Cobertura de seguro

A AC TrustSign deverá manter, a expensas próprias, Comércio Seguro de Responsabilidade Civil Geral, com um limite suficientemente elevado para a condução de seus negócios. O seguro deve cobrir as responsabilidades resultantes de instalações, operações, fornecedores independentes, produtos de operações concluídas, lesões corporais e danos de publicidade e responsabilidade assumida no âmbito de um contrato de seguro.

9.2.2 Outros ativos

Não estipulado

9.2.3 Cobertura de seguro ou garantia para entidades

A AC TrustSign não é um administrador, agente fiduciário, ou outro representante do Assinante e as relações entre TrustSign CA eo Assinante não é a de um agente e / ou principal. A AC TrustSign não faz nenhuma representação ao contrário, de forma implícita, explicitamente, pela aparência ou não. O assinante não possui autoridade para vincular a CA TrustSign por contrato, acordo ou não, de qualquer obrigação.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

9.3 Confidencialidade de informações comerciais

9.3.1 Escopo de informações confidenciais

Pessoais e informações corporativas, que não figuram nos certificados e em listas públicas, realizado pela TrustSign CA (por exemplo, registro e informações de revogação, os eventos registrados, a correspondência entre Assinante e TrustSignCA) são consideradas confidenciais e não serão divulgadas pelA AC TrustSign. Assinante informações confidenciais não serão divulgadas sem o consentimento prévio do assinante a menos que exigido por lei.

As informações de auditoria são consideradas confidenciais e não serão divulgadas a qualquer um para qualquer outro fim que não fins de auditoria ou quando exigido por lei, ou de um acordo contratual entre A AC TrustSign ea empresa a ser dado acesso ao relatório que protege a confidencialidade das informações de auditoria .

As informações relativas a TrustSign gestão do CA de um certificado de assinatura digital do assinante só poderão ser divulgados ao Assinante ou quando exigido por lei.

Qualquer pedido de divulgação de informações devem ser assinados e entregues por escrito à Autoridade de Certificação emissora.
Qualquer divulgação de informações está sujeita às exigências de todas as leis de privacidade, o RSA ROOT a assinatura de serviço Política de Privacidade e qualquer outra legislação pertinente e política organizacional aplicável.

* Assinatura *
A chave privada de assinatura digital de cada assinante, deve ser realizada apenas pelo Assinante e serão mantidas em sigilo por eles. Qualquer divulgação da chave privada ou mídia contendo a chave privada do assinante é por conta e risco do Assinante.

* CONFIDENCIAL
O assinante deve manter cópia do Assinante confidencialidade de sua chave privada e confidencial. Divulgação pelo Assinante é por conta e risco do Assinante. teclas de sigilo pode ser acompanhada pela emissão TrustSign CA, caso em que estas chaves devem ser protegidos de acordo com o ponto 6, e não devem ser divulgadas sem prévia autorização do assinante ou por um representante devidamente autorizado da CA de emissão a menos que exigido por lei.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

9.3.2 Informação fora do escopo de informações confidenciais

Certificados, LCR, as respostas OCSP (se aplicável) e informações pessoais ou de empresas que aparecem nelas e nas listas públicas não são consideradas informações confidenciais. Além disso, a informação que atenda aos seguintes critérios não devem ser consideradas informações confidenciais:
1. Informação que é documentado pela parte que recebe como tendo sido desenvolvida de forma independente por ela sem referência não autorizado ou a confiança na informação confidencial da parte reveladora;
2. As informações que a parte que recebe legalmente recebe livre de restrições a partir de uma fonte diferente da parte divulgadora;
3. Informação que é ou passa a estar disponível ao público através de nenhum ato doloso ou omissão por parte da festa de recepção;
4. Informação que, no momento de divulgação para a festa era conhecido por receber da parte receptora sem restrições quanto comprovado por documentação na posse da parte receptora, ou
5. Informação que a parte divulgadora concorda em escrever é livre de restrições.

9.3.3 Responsabilidade em proteger informações confidenciais

TrustSign CA garante que informações confidenciais sejam fisicamente e / ou logicamente protegido contra visualização não autorizada, modificação ou eliminação. Além disso, o CA deve assegurar que os meios de armazenamento utilizado pelo sistema CA está protegido contra ameaças ambientais, como temperatura, umidade e magnetismo.
chaves de confidencialidade são apoiadas pela emissão TrustSign CA, caso em que estas chaves são protegidos nos termos da secção 6, e não sejam divulgados sem o consentimento prévio do assinante ou por um representante devidamente autorizado da CA de emissão a menos que exigido por lei.

9.4 Privacidade da informação pessoal

A TrustSign AC raiz não processa todos os dados pessoais, exceto para o seguinte:
 Os endereços de e-mail dos Diretores e Gerentes TrustSign de Segurança da CA. Estes não são publicados e são utilizados apenas para anúncios referentes aA AC TrustSign. TrustSign CA publica um endereço de e-mail genérico para manter contato com Oficiais TrustSign Segurança: ouvidoria@TrustSign.com.br

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

9.4.1 Plano de Privacidade

O princípio orientador TrustSign CA é para não divulgar informações pessoais privadas de seus assinantes, clientes, colaboradores e parceiros, sem o consentimento prévio do referido exceto se exigido por lei.

9.4.2 Informações tratadas como privada

As informações pessoais que não constam em certificados e em listas públicas, realizado por uma CA TrustSign (Ex. registro e informações de revogação, os eventos registrados, e correspondência entre Assinante e TrustSign CA) é considerado privado, e não devem ser divulgadas pelo CA theTrustSign.

9.4.3 Informação não considerada privada

As informações pessoais que estão disponíveis publicamente, aparecendo em certificados e em listas públicas, não é considerada privada.

9.4.4 Responsabilidade em proteger informações privadas

TrustSign CA garante que a informação pessoal privada são fisicamente e logicamente protegido contra visualização não autorizada, modificação ou eliminação. Além disso, a CA garante que TrustSign mídia de armazenamento utilizado pelo sistema CA TrustSign está protegido contra ameaças ambientais, como temperatura, umidade e magnetismo como descrito na seção 5 .

9.4.5 Notificação e consentimento de uso de informações privadas

Informação pessoal privada será apenas utilizada sem o consentimento prévio acordo com o ponto 9.4.1.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

9.4.6 Divulgação por força de processo judicial ou administrativo

A informação privada só será divulgada se exigido por lei conforme a secção 9.4.1.
Qualquer pedido de divulgação de informação privada deve ser assinado pelo solicitante e entregue por escrito à CA TrustSign. Qualquer divulgação de informação privada está sujeita aos requisitos de todas as leis de privacidade e demais legislação pertinente e política organizacional aplicável.

9.4.7 Outras circunstâncias de divulgação de informações

Não estipulado.

9.5 Direitos de propriedade intelectual

A chave privada de assinatura será de propriedade exclusiva do legítimo titular da chave pública correspondente identificadas em um certificado.
Qualquer pessoa pode copiar livremente a partir de qualquer versão de Certificação da CA TrustSign de Declaração de Práticas, desde que incluam um reconhecimento dessas fontes.
TrustSign mantém todos os direitos de propriedade intelectual e, para o DPC.

9.6 Representações e garantias

TrustSign CA irá emitir e revogar certificados, operar a sua certificação e serviços de repositório e fornecer informações de status de certificado em conformidade com esta PC.
Os procedimentos de autenticação e validação serão aplicadas conforme estabelecido na Seção 3 do CP.

9.6.1 Representações e garantias da AC

TrustSign CA irá operar de acordo com esta CP / DPC e as leis aplicáveis, conforme descrito na Seção 2.4.1, salvo disposição em contrário da raiz assinatura do contrato, quando da emissão e gerenciamento de certificados fornecidos a TrustSign CA. TrustSign CA irá tomar medidas comercialmente razoáveis para fazer Assinantes e Partes Confiantes conscientes dos seus direitos e obrigações no que diz respeito à operação e gestão de todas as chaves, certificados ou hardware da entidade final e software usado em conexão com a PKI. Os assinantes também devem ser notificados quanto aos procedimentos para lidar com suspeita de comprometimento da chave, certificado ou renovação de chaves, e cancelamento de serviço.
TrustSign CA deve fornecer um aviso de qualquer limitação de responsabilidade (Seção 2.2). Esse aviso pode, no mínimo, ser fornecido dentro do certificado através de uma extensão de certificado privado ou o uso do "userNotice" campo dentro do certificado definido pela PKIX.
Quando TrustSign CA publica ou fornece um certificado, ele declara que tenha emitido um certificado para um assinante e que a informação constante do certificado foi verificada em conformidade com a presente CP / DPC.
pessoal TrustSign CA associado a papéis PKI devem ser individualmente responsável pelas ações que realizam.
"Individualmente responsáveis" significa que não possa ser comprovado que os atributos de uma ação para a pessoa que executa a ação.
Ao emitirem um certificado para uma CA Assunto, a CA TrustSign terá avaliado o CP / DPC da CA assunto e está convencida de que o CA Assunto, quando estiver operando de acordo com seu CP / DPC, em conformidade com as exigências impostas por este documento .

9.6.2 Representações e garantias da AR

A AC TrustSign devem exigir que RAs executar tarefas de registro de Assinante, em seu nome, cumprir todas as disposições pertinentes da RSA RSS CP, esta DPC e outras aplicações TrustSign e documentação serviços esboçando requisitos TrustSign.
A AR é responsável pela identificação, autenticação e autorização de assinantes, em nome da AC TrustSign como descrito na secção 3.1 e secção 4.1 desta DPC, para solicitações de certificado e os pedidos de revogação de certificado.
RA devem ser individualmente responsável pelas ações realizadas em nome da TrustSign CA. Individualmente responsabilização significa que deve haver provas (logs de auditoria), que atribui uma ação à pessoa que realiza a ação. Os registros de todas as ações realizadas no exercício de funções RA deve identificar o indivíduo que realizou o dever particular.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

Quando um RA apresenta informações Assinante de uma CA TrustSign, deve certificar que a CA que tem autenticados a identidade do assinante e que o Assinante está autorizado a apresentar um pedido de certificado em conformidade com o ponto 3 e ponto 4.

9.6.3 Representações e garantias do Assinante

Assinantes registrar e aceitar um certificado da CA TrustSign será obrigado a concordar com um acordo de Assinantes.
Assinantes declara e garante que qualquer informação Assinante (ou seja, os dados necessários para a construção ou certificado de um repositório de dados ou fornecidos pelo assinante na página da inscrição) devem ser completos e validados com a divulgação integral de todas as informações exigidas no âmbito de um pedido de certificado.

9.6.4 Representações e garantias de Terceiros de Confiança

Partes Confiantes deve ler e concordar com todos os termos e condições de qualquer acordo de participação dos associados do serviço TrustSign.

9.6.5 Representações e garantias de outros participantes

Não estipulado.

9.7 Isenção de responsabilidades

A AC TrustSign não assume qualquer responsabilidade, salvo como previsto nos respectivos contratos relativos à emissão de certificados e de gestão, como um Acordo de Subscrição ou de outros acordos de serviços relevantes.
Em nenhum caso A AC TrustSign ser responsabilizada por qualquer das partes, por quaisquer danos incidentais, conseqüentes, especiais, indiretos ou punitivos, lucros cessantes negócio, ou perda, dano ou destruição de dados resultante de ou relacionado de alguma forma para os certificados emitidos por CA TRUSTSIGN, independentemente da forma de actuação, quer em contrato, ilícito (incluindo negligência), violação da

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

garantia, ou não, mesmo que a CA TRUSTSIGN tenha sido avisada da possibilidade de o mesmo.
Nada na DPC da AC TrustSign confere a terceiros qualquer autoridade para agir, ligar, ou criar ou assumir qualquer obrigação ou responsabilidade, ou fazer qualquer representação em nome do outro, exceto conforme estipulado no contrato em causa. Emissão de certificados de acordo com esta política não faz um CA ou RA um agente, parceiros, associados, administrador, fiduciário ou outro representante dos assinantes, clientes ou outras partes Confiantes. A relação entre a CA, RA e qualquer Assinante é definido pelo contrato em vigor.
As isenções estão sujeitas a qualquer contrato assinado, que podem ser introduzidos pela CA TrustSign que disponha em contrário. Qualquer negação ou limitação de responsabilidade será compatível com o RSS RSA PB e do acordo assinado pela TrustSign e RSA.

9.8 Limitações de responsabilidade

Em nenhum caso A AC TrustSign se responsabiliza por quaisquer danos aos Assinantes, Partes Confiantes ou qualquer outra parte decorrentes ou relacionados ao mau uso, ou confiança dos certificados emitidos pela CA que tenham sido:

(I) Revogado ou expirado;
(Ii) Utilizado para fins não autorizados;
(Iii) Adulterado;
(Iv) Comprometido;
(V) Sujeito a falsas declarações, atos ou omissões enganosas.
As limitações de responsabilidade estão sujeitos a qualquer contrato assinado, que podem ser introduzidos pela CA TrustSign que disponha em contrário. Qualquer negação ou limitação de responsabilidade será compatível com o RSS RSA PB e do acordo assinado pela TrustSign e RSA.

9.9 Indenizações

Salvo disposição em contrário estabelecida no RSS RSA CP, esta DPC, quaisquer Assinante ou qualquer parte relevante Parte Confiante acordo, assinante e / ou Confiando concorda em indenizar e defender TrustSign CA e seus administradores, diretores, agentes e empregados de qualquer reivindicações, ações ou demandas que são causados por ou resultantes do uso ou publicação de um certificado, incluindo mas não limitado a, reivindicações, ações e demandas que surgem a partir de:

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

1. Qualquer declaração falsa ou enganosa de facto do Assinante;
2. Qualquer falha por parte do Assinante em divulgar um fato relevante, se essa omissão foi feita de forma negligente ou com a intenção de enganar;
3. Qualquer falha por parte do assinante para proteger sua chave privada e / ou ficha se for o caso, ou de tomar as precauções necessárias para impedir o comprometimento, a divulgação, perda, modificação ou uso não autorizado da chave privada do Assinante, ou
4. Qualquer falha por parte do assinante para notificar imediatamente o CA da TrustSign, a divulgação de compromisso, a perda, modificação ou uso não autorizado da chave privada do assinante uma vez que o assinante tem notícia real ou construtiva de tal evento.

9.10 Prazo e terminação

9.10.1 Prazo

Esta DPC se mantém em vigor até novo aviso, do contrário será comunicada por TrustSign em seu site (www.TrustSign.com.br), sem aviso prévio.

9.10.2 Terminação

A denúncia do presente documento será mediante a publicação de uma versão mais recente ou documento de substituição, ou após o término das operações TrustSign CA.

9.10.3 Efeito de terminação e sobrevivência

As condições e os efeitos resultantes da rescisão do presente documento será comunicado, no ponto de publicação TrustSign CA DPC, com o término delineando as disposições que podem sobreviver a sua rescisão e permanecem em vigor.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

9.11 Notificações individuais e comunicações aos participantes

Todos os acordos entre a CA TrustSign e qualquer organização deve ser documentada e assinada pelas autoridades competentes. Uma lista de discussão deve ser mantida para anúncios referentes aA AC TrustSign.

9.12 Emendas

TrustSign Security Management Team é a autoridade responsável pela análise e aprovação de alterações a esta DPC. comentários por escrito e assinado em alterações propostas devem ser encaminhadas para o contatA AC TrustSign conforme descrito na Seção 1.5. As decisões com relação às mudanças propostas estão a critério do Conselho de Segurança TrustSign Equipa de Gestão.

9.12.1 Procedimento para emendas

Uma cópia eletrônica do TrustSign CA DPC está a ser disponibilizado no site da TrustSign (www.TrustSign.com.br) ou solicitando uma cópia eletrônica por e-mail para contato com o representante, conforme descrito na Seção 1.5.
O TrustSign Security Management Team pode notificar, por escrito, de quaisquer alterações propostas para a sua DPC, se no julgamento e discrição do TrustSign Security Management Team mudanças podem ter impacto significativo sobre os certificados emitidos e serviços TrustSign.
O período de tempo em que as partes envolvidas têm que estar em conformidade com a alteração será definido na notificação.

9.12.2 Mecanismo de notificação e período

A notificação deve conter uma declaração de alterações propostas, a data limite para a recepção de comentários, a data proposta efetiva de mudança. A AC TrustSign vou postar a notificação, o ponto de publicação TrustSign CA DPC.
O período de comentários será de 30 dias, salvo indicação em contrário. O período para comentários serão definidos na notificação.

9.12.3 As circunstâncias sob as quais o OID deve ser alterado

Se uma mudança de política é determinada pela RSA ROOT a assinatura de serviço para autorizar a emissão de uma nova política, a RSA ROOT a assinatura de serviço irá atribuir uma nova Object Identifier (OID) para a nova política e notificar a AC TrustSign.

9.13 Procedimentos na Solução de Disputas

Qualquer controvérsia relativa à chave eo certificado de gestão entre a CA TrustSign e qualquer outra organização ou indivíduo fora do CA deve ser resolvido através de um mecanismo de resolução de litígios adequado, se possível. As partes concordam em tentar resolver qualquer litígio primeiro por meio de negociações informais, conforme descrito abaixo, a menos que medidas cautelares ou imediata é necessária. A AC TrustSign irá fornecer procedimentos adequados de resolução de litígios em qualquer contrato em que se insere. Se não existe um procedimento de resolução de litígios no acordo, então esta seção do DPC terá prioridade.

9.13.1 Negociação

A AC TrustSign e seu cliente tentará resolver qualquer controvérsia relativa a um acordo, referente a esta DPC ou declarações associadas de trabalho através de negociações entre representantes dos partidos que têm a autoridade para resolver a controvérsia. Esses representantes serão nomeados no momento do contrato, juntamente com uma designação. Um aviso escrito, indicando as controvérsias e a providência requerida deve ser fornecida. Este aviso deve ser datado e assinado pelo representante designado. Toda a correspondência deve ser mantido a um máximo de 3 (três) páginas.
A parte litigante vai notificar por escrito a outra parte do litígio. No prazo de 5 (cinco) dias úteis a parte que recebe apresentará à resposta de um outro escrito (máximo 3 páginas). Os representantes nomeados irão reunir-se em um tempo acordado e num prazo de cinco (5) dias úteis a partir da data da notificação da parte receptora. O objetivo do encontro é negociar a resolução do litígio.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

9.13.2 Mediação

No caso de a negociação falhar ao resolver o litígio no prazo de 30 (trinta) dias, a disputa será submetida à mediação. O mediador não tem poder para obrigar as partes. A mediação será confidencial e sem preconceitos.
1. Seleção do Mediador - Ambas as partes terão três dias para chegar a acordo sobre um mediador mutuamente aceitável. Se nenhum mediador foi selecionado ambas as partes concordam em solicitar um local Alternative Dispute Resolution (ADR) Service Provider para fornecer uma lista de cinco (5) potenciais mediadores. Ambas as partes concordam em escolher um dos cinco candidatos.
2. Tempo e lugar para a mediação - Ambas as partes, em consulta com o mediador, vai concordar em um tempo e lugar comum para a mediação. A data será definida no prazo de cinco (5) dias úteis após a escolha do mediador.
3. Taxas de mediador - Os honorários do mediador será repartido em partes iguais por ambas as partes.
4. Encerramento do processo - Ambas as partes concordam em participar da mediação, pelo menos, 4 (quatro) horas. Após esse tempo, qualquer das partes pode deixar a mediação a qualquer momento. Se a mediação não se rende a um acordo, em seguida, ambas as partes concordam em não tomar qualquer outra medida que as tentativas de boa fé para negociar uma solução do litígio antes de um período de cinco a mediação de pós-(5) dias.

9.13.3 Arbitragem ou litígio

No caso de as negociações e mediação falhar, então ambas as partes podem convencionar a arbitragem ou litígio.
Arbitragem - Em caso de acordo sobre arbitragem ambas as partes terão cinco (5) dias úteis a partir da final do período pós-mediação para chegar a acordo sobre um árbitro. Ambas as partes, em consulta com o árbitro concordar com as regras de arbitragem.
Litígio - No caso de qualquer uma das partes decida pleitear, contencioso deve ser interposto perante o tribunal de TBD, ou conforme estipulado no acordo.

9.14 Leis Vigentes

A AC TrustSign e sua operação estão sujeitas à legislação pertinente em vigor na República Federativa do Brasil, e sem entrar em conflito com os princípios das Nações Unidas de 1980 Convenção sobre Contratos para a Venda Internacional de Mercadorias leis.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

Ele é o eleito do condado Foro de São Paulo como a competência para resolver conflitos e dúvidas vêm desta DPC, com exclusão de qualquer outro, porém, pode ser.
Estado clientes que utilizam apenas os certificados emitidos pela TrustSign em estrita conformidade com as leis aplicáveis e os termos desta DPC.

9.15 Conformidade com a legislação aplicável

Não estipulado.

9.16 Disposições variadas

9.16.1 Contrato completo

Esta DPC e as políticas e procedimentos promulgados pelA AC TrustSign EM CONEXÃO constituem o completo entendimento e acordo com relação a este assunto, e substituem todos e quaisquer anteriores ou atuais declarações, entendimentos e acordos orais ou escritos entre um assinante e TrustSign CA relacionadas ao assunto desta DPC, que são mescladas nesta DPC ..

9.16.2 Atribuição

Assinantes e Partes Confiantes não pode ceder nenhum dos seus direitos ou obrigações contratuais, sem o consentimento por escrito da TrustSign CA.

9.16.3 Severidade

No caso de qualquer disposição desta DPC é considerada inválida ou inexeqüível nos termos do decreto ou decisão judicial, o restante desta DPC deverá permanecer válido e exeqüível de acordo com estes termos, a menos que devido a tal nulidade, uma parte é negado um material benefícios que adviriam tinha a disposição não foi considerada inválida.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

9.16.4 Aplicação (honorários advocatícios e renúncia de direitos)

A AC TrustSign definirá, em qualquer acordo, as disposições adequadas relativas à execução.

9.16.5 Força maior

A AC TrustSign não será responsabilizado por qualquer atraso ou falha no desempenho de suas obrigações aqui à medida em atraso ou falha é causada por incêndio, inundação, greve, entidade civil, governamental ou militar, atos de terrorismo ou de guerra, ato de Deus, ou outras causas semelhantes fora de seu controle razoável, sem culpa ou negligência da parte atrasada ou não-realização ou seus subcontratados

9.17 Outras disposições

Não estipulado.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

10 GLOSSÁRIO

TERMO: Autoridade de Registro
DEFINIÇÃO: Uma entidade aprovada por uma AC, a auxiliar Solicitantes de Certificado na inscrição para certificados, bem como funções de aprovação ou rejeição de Solicitações, revogação e renovação de Certificados.

TERMO: Controle de Acesso
DEFINIÇÃO Permissão ou negação de uso ou entrada.
TERMO: Dados de Ativação
DEFINIÇÃO: Uma parte de uma chave privada de AC ou parte dos dados de ativação necessários para operar uma chave privada de AC conforme acordo Secret Sharing..

TERMO: Administrador
DEFINIÇÃO: Um administrador que executa funções de validação e outras funções de AR para um Cliente
TERMO: Autenticação
DEFINIÇÃO: Procedimento onde as Solicitações de Certificado são avaliadas e aprovadas
TERMO: Autorização
DEFINIÇÃO: A permissão de uso ou acesso.
TERMO: Certificado
DEFINIÇÃO: Uma mensagem que ao menos define o nome ou identifica a AC, identifica o Assinante, contém a chave pública do Assinante, identifica o Período Operacional do Certificado, contém um número de série do Certificado e é digitalmente assinado pela AC.

TERMO: Autoridade Certificadora (AC)
DEFINIÇÃO: Uma autoridade confiável por um ou mais usuários para gerenciar Certificados X.509 e LCRs.
TERMO: Declaração de Práticas de Certificação
DEFINIÇÃO: Uma declaração das práticas que a TrustSign emprega na aprovação ou rejeição de Solicitações de Certificados, e para a emissão, gerenciamento, revogação de Certificados e requer que seus Clientes de PKI Gerenciada a empreguem..

TERMO: Lista de Certificados Revogados – LCR ou CRL
DEFINIÇÃO: Uma lista emitida periodicamente (ou conforme demanda), assinada digitalmente por uma AC, de um Certificado identificado que foi revogado antes de suas datas de vencimento de acordo com a PC§ 3.4. A lista geralmente indica o nome do emissor da CRL, os números de série do Certificado revogado e os horários e motivos específicos para a revogação.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948

TERMO: Certificados de e-mail
DEFINIÇÃO: Certificados utilizados para criptografare verificar a assinatura digital. Normalmente há dois certificados separados, um para criptografia e outro para verificação e assinatura.
TERMO: PKCS #10
DEFINIÇÃO: Public-Key Cryptography Standard #10, desenvolvido pela RSA Security Inc., que define uma estrutura para uma Solicitação de Assinatura de Certificado\..

TERMO: Repositório
DEFINIÇÃO: Banco de dados da TrustSign e outras informações relevantes da AC acessíveis online.

TERMO: RSA
DEFINIÇÃO: Chave criptográfica pública inventada por Rivest, Shamir, e Adelman..
TERMO: Secure Sockets Layer (SSL)
DEFINIÇÃO: Método padrão da indústria para proteger as comunicações via Internet, foi desenvolvida pela Netscape Communications Corporation. protocolo de segurança SSL oferece a criptografia de dados, autenticação de servidor, integridade de mensagem e autenticação cliente opcional para uma conexão TCP/IP.

Tel SP (11) 3729-3945 | Tel SJC (12) 3308-8422 |Fax (11) 3729-3948